Пусть случайная величина К - произвольно распределена на $\mathcal{K}$

воспоминания о выпуклостях

Пусть функция φ выпукла вниз на отрезке $[a,\ b]$, то есть

$$a \le x < y \le b: \ \forall\ z \in [x,\ y]: \ \varphi(z) \le \varphi(x) + \frac{\varphi(y)-\varphi(x)}{y-x}(z-x).$$

Рис. 1: alt text

Неравенство Йенсена

Если f(x) - выпукла на [a,b]
Тогда $\forall \vec{\alpha} = (\alpha_1, \alpha_2 \cdots \alpha_k)$ -стохастического вектора, $\forall x_1, x_2, \cdots x_k \in [a,b]:$

$$f(\sum_{i=1}^{k} \alpha_i \cdot x_i) \le \sum_{i=1}^{k} \alpha_i \cdot f(x_i)$$

Д-ВО

Первая база индукции k = 1
$f(x_1) = f(x_1)$
Вторая база индукции k = 2

Обязательно ли нужно показывать вторую базу, если есть первая

Б.Б.О $x_1 < x_2$
т.е надо показать что

$$f(\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2) \le \alpha_1 \cdot f(x_1) + \alpha_2 \cdot f(x_2)$$

- очевидно что:

$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_1 < \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 < \alpha_1 \cdot x_2 + \alpha_2 \cdot x_2$
где

- $\alpha_1 \cdot x_1 + \alpha_2 \cdot x_1 = x_1$
- $\alpha_1 \cdot x_2 + \alpha_2 \cdot x_2 = x_2$

пусть тогда $\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 = x$. получаем, что $x_1 < x < x_2$
пусть

- $\alpha_1 = \alpha$
- $1 - \alpha = \alpha_2$

т.к f(x) - выпукла, то:
$f(x) \le f(x_1) + \frac{(f(x_2) - f(x_1))}{x_2 - x_1} \cdot (x - x_1)$

- где $(x - x_1) = (1 - \alpha) \cdot (x_2 - x_1)$

$f(x) \le f(x_1) + (f(x_2) - f(x_1)) \cdot (1 - \alpha) =$
$\alpha_1 \cdot f(x_1) + \alpha_2 \cdot f(x_2)$
Ш.И $k \to k+1$
нужно доказать $f(\alpha_1 x_1 + \cdots + \alpha_k x_k + \alpha_{k+1} x_{k+1}) \le \alpha_1 f(x_1) + \cdots \alpha_k f(x_k) + \alpha_{k+1} f(x_{k+1})$
Сделаем переобозначение для иксов

- $y_1 = x_1$
- $y_2 = x_2$
- $\cdots$
- $y_k = x_k$
- $y_{k+1} = \frac{\alpha_k x_k + \alpha_{k+1} x_{k+1}}{\alpha_k + \alpha_{k+1}}$

заметим,что $(\frac{\alpha_k}{\alpha_k + \alpha_{k+1}}, \frac{\alpha_{k+1}}{\alpha_k + \alpha_{k+1}})$ - стохастический вектор точка $y_k \in [x_k, x_{k+1}] \Rightarrow y_k \in [a,b]$

теперь переобозначаем альфы

- $\beta_1 = \alpha_1$
- $\beta_2 = \alpha_2$
- $\cdots$
- $\beta_{k-1} = \alpha_{k-1}$
- $\beta_k = \alpha_k + \alpha_{k-1}$

тогда $(\beta_1, \cdots \beta_k)$ - стохастический вектор

По П.И имеем неравенство $f(\alpha_1 x_1 + \cdots + \alpha_k x_k) \leq \alpha_1 f(x_1) + \cdots \alpha_k f(x_k) = f(\beta_1 y_1 + \cdots + \beta_k y_k)$

$\beta_1 \cdot f(y_1) + \cdots + \beta_{k-1} f(y_{k-1}) + \beta_k f(y_k) =$

$\alpha_1 \cdot f(x_1) + \cdots + \alpha_{k-1} f(x_{k-1}) + (\alpha_k + \alpha_{k+1}) f(\frac{\alpha_k x_k}{\alpha_k + \alpha_{k+1}} + \frac{\alpha_{k+1} x_{k+1}}{\alpha_k + \alpha_{k+1}}) =$

- по Б.И № 2 и используем Ш.И для $(\frac{\alpha_{k+1} x_{k+1}}{\alpha_k + \alpha_{k+1}})$

$\alpha_1 \cdot f(x_1) + \cdots + \alpha_{k-1} f(x_{k-1}) + \alpha_k f(x_k) + \alpha_{k+1} f(x_{k+1})$

■

Утверждение 3

$log(P_{\text{им}}) \geq -I(K \leftrightarrow C)$

Д-ВО

пусть $c \in \mathcal{C}$ - допустимая, если $D(c,k) \in \mathcal{M}$, где k - это ключ, который сейчас используют A и B

$0 \leq P(c - \text{допустимая}) = \sum\limits_{k \in \mathcal{K}} P(c - \text{допустимая} | K = k) \cdot P(K = k) =$

- если ключ известен, то $P(c - \text{допустимая}|K = k)$ либо 0 либо 1.

$\delta(c,k) = \begin{cases} 1, D(c,k) \in \mathcal{M} \\ 0, D(c,k) \notin \mathcal{M} \end{cases}$

$\sum\limits_{k \in \mathcal{K}} P(c - \text{допустимая}|K = k) \cdot P(K = k) \cdot \delta(c,k) =$

- если щас уберем $P(c - \text{допустимая}|K = k)$ то ничего не изменится, т.к умножили на $\delta(c,k)$
- $\delta(c,k)$ это и есть $P(c - \text{допустимая}|K = k)$

$\sum\limits_{k \in \mathcal{K}} P(K = k) \cdot \delta(c,k) =$

$\measuredangle Q_c(k) = \frac{P(K=k) \cdot \delta(c,k)}{P(c - \text{допустимая})}$

Вектор $(Q_c(K) | k \in \mathcal{K})$ - стохастический.

$P(C = c) = \sum\limits_{k \in \mathcal{K}} P(C = c|K = k) \cdot P(K = k) =$

- Домножаем на $\delta(c,k)$. После домножения ничего не меняется

$\sum\limits_{k \in \mathcal{K}} P(C = c|K = k) \cdot P(K = k) \cdot \delta(c,k) =$

- подставляем $Q_c(k)$

$P(c - \text{допустимая}) \cdot \sum\limits_{k \in \mathcal{K}} P(C = c|K = k) \cdot Q_c(k) =$

$\forall c \in \mathcal{C} \measuredangle\ P(C = c) \cdot log(P(C = c)) =$

$P(C = c) \cdot log(P(c - \text{допустимая})) + P(C = c) \cdot log(\sum\limits_{k \in \mathcal{K}} P(C = c|K = k) \cdot Q_c(k)) =$

- распишем $P(C = c)$ у правого множителя

$P(C = c) \cdot log(P(c - \text{допустимая})) + (P(c - \text{допустимая}) \cdot \sum\limits_{k \in \mathcal{K}} P(C = c|K = k) \cdot Q_c(k)) \cdot log(\sum\limits_{k \in \mathcal{K}} P(C = c|K = k) \cdot Q_c(k)) \leq$

- функция $t \cdot log(t)$ выпукла вниз, поэтому используем н-во йенсена

$P(C = c) \cdot log(P(c - \text{допустимая})) + P(c - \text{допустимая}) \cdot \sum\limits_{k \in \mathcal{K}} Q_c(k) P(C = c|K = k) log(P(C = c|K = k)) =$

- подставили $Q_c(k)$

$P(C = c) \cdot log(P(c - \text{допустимая})) + \sum\limits_{k \in \mathcal{K}} \delta(c,k) \cdot P(K = k) \cdot P(C = c|K = k) log(P(C = c|K = k)) =$

- $P(K = k) \cdot P(C = c|K = k) = P(C = c, K = k)$
- можем стереть $\delta(c,k)$, т.к если оно 1, то ничего не изменится, а если оно 0, то $P(C = c|K = k) = 0$

$P(C = c) \cdot log(P(c - \text{допустимая})) + \sum\limits_{k \in \mathcal{K}} P(K = k, C = c) \cdot log(P(C = c|K = k)) =$

- В итоге получаем $\forall c \in \mathcal{C}$ н-во:

$$P(C=c)\cdot log(P(C=c)) \leq$$

$$P(C=c)\cdot log(P(c-\text{допустимая})) + \sum_{k\in\mathcal{K}} P(K=k, C=c)\cdot log(P(C=c|K=k))$$

- складываем это н-во по всем $c \in \mathcal{C}$

$\sum\limits_{c\in\mathcal{C}} P(C=c)\cdot log(P(C=c)) \leq$
$\sum\limits_{c\in\mathcal{C}} P(C=c) log(P(c-\text{допустимая})) + \sum\limits_{c\in\mathcal{C}}\sum\limits_{k\in\mathcal{K}} P(K=k, C=c) log(P(C=c|K=k))$

- $\sum\limits_{c\in\mathcal{C}} P(C=c)\cdot log(P(C=c)) = -H(C)$
- $\sum\limits_{c\in\mathcal{C}}\sum\limits_{k\in\mathcal{K}} P(K=k, C=c) log(P(C=c|K=k)) = -H(C|K)$

$-H(C) \leq \sum\limits_{c\in\mathcal{C}} P(C=c) log(P(c-\text{допустимая})) - H(C|K) \leq$

- оценили $log(P(c-\text{допустимая})) \leq \max\limits_{c\in\mathcal{C}}\{log(P(c-\text{допустимая}))\}$

$\sum\limits_{c\in\mathcal{C}} P(C=c) \max\limits_{c\in\mathcal{C}}\{log(P(c-\text{допустимая}))\} - H(C|K) \leq$

- т.к логорифм функция возрастающая, то максимум логорифма это логорифм максимума

$log\{\max\limits_{c\in\mathcal{C}} P(c-\text{допустимая})\} \cdot \sum\limits_{c\in\mathcal{C}} P(C=c) - H(C|K) =$

- $\max\limits_{c\in\mathcal{C}} P(c-\text{допустимая}) = P_{\text{им}}$
- $\sum\limits_{c\in\mathcal{C}} P(C=c) = 1$

$log(P_{\text{им}}) - H(C|K)$
В итоге получаем, что:

$$H(C|K) - H(C) \leq log(P_{\text{им}})$$

- применяем цепное правило к H(C|K)
- Используем терему о взаимной информации

$H(C,K) - H(K) - H(C) = I(C \leftrightarrow K)$
■

Смысл утверждения 3

Чтобы уменьшить $P_{\text{им}}$ надо увеличить $I(K \leftrightarrow C)$.
$I(K \leftrightarrow C)$ - мера того, в какой степени ключ используется для защиты от атаки имитации.

ОПР (шифр совершенной имитационной стойкостью)

Шифр обладает совершенной имитационной стойкостью, если $log(P_{\text{им}}) = -I(K \leftrightarrow C) \Rightarrow P_{\text{им}} = (\frac{1}{2})^{I(K\leftrightarrow C)}$