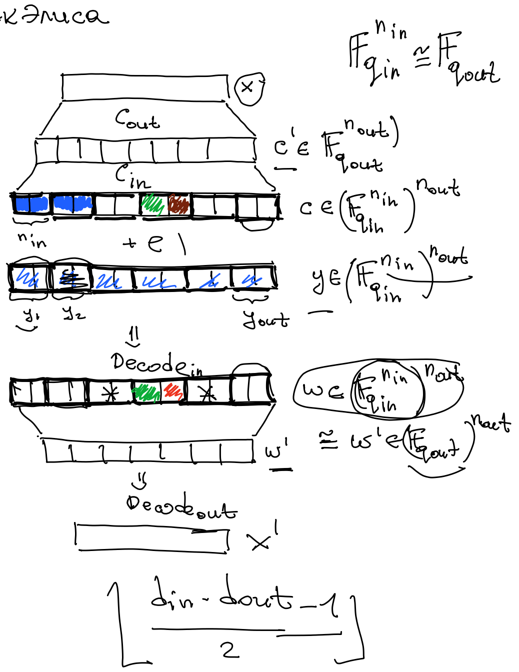
Лекция №12 Коды конкатенации II. Криптосистема МакЭлиса

Tuesday 17 November 2020 11:11



Напоминание

Алгоритм Форней (Forney)

Вход: $(y_1,\dots,y_{out}) \in (\mathbb{F}_{q_{in}}^{n_{in}})^{n_{out}}$

фикс. θ

1) для $i = 1 \dots n_{out}$

1.1. $w_i = \arg\min_{c \in C_{in}} \Delta(y_i, c) \in \mathbb{F}_{q_{in}}^{n_{in}}$ } декодирование по синдрому

1.2. С вероятностью $\min\{1, \frac{2\Delta(y_i,w_i)}{d_{in}}\}$

Если $2\Delta(y_i,w_i)/d_{in} > \theta$

$w_i' =$ "$*$"

иначе

w_i' т.ч. $Encode_{in}(w_i') = w_i$

2) $x' = Decode_{out}(w_1', \dots, w_{n_{out}}')$, $w_i' \in \mathbb{F}_{q_{out}} \cup \{"*"\}$

вернуть x'

Корректность

Предложение $\underbrace{\mathbb{E}}_{\text{случайность алгоритма}}\left[\,|w_i' = "*"| + 2|w_i' \notin C_{out}|\,\right] \le d_{out}$.
(по лемме, шаг 2 будет успешен "в среднем")

◄ $e_i = \Delta(y_i, c_i)$

$wt(e) = \sum e_i < \frac{d_{in}\cdot d_{out}}{2}$

обозначим $\forall i \le n_{out}$ $Z_i^{erasure} = \begin{cases} 1, & w_i' = '*' \\ 0, & \text{иначе} \end{cases}$; $Z_i^{error} = \begin{cases} 1, & w_i' \ne "*" \text{ и } c_i \ne w_i \\ 0 \end{cases}$

утверждение $\mathbb{E}\left[2\cdot Z_i^{error} + Z_i^{erasure}\right] \le \frac{2e_i}{d_{in}}$ (1)

из (1) $\Rightarrow$ предложение,

т.к. $\mathbb{E}\left[\sum_i Z_i^{erasure} + 2\sum_i Z_i^{error}\right] = \sum_{i \le n_{out}} \mathbb{E}\left[Z_i^{erasure} + 2Z_i^{error}\right]$

$\le \sum_{i \le n_{out}} 2\frac{e_i}{d_{in}} < \frac{2}{d_{in}} \cdot \frac{d_{in}\cdot d_{out}}{2} = d_{out}$

Случай 1 $w_i = c_i$; $Z_i^{error} = 0$

$\mathbb{E}\left[Z_i^{erasure}\right] = 0 \cdot \Pr[Z_i^{erasure} = 0] + 1 \cdot \Pr[Z_i^{erasure} = 1]$

$= \min\{1, \frac{2\Delta(y_i,w_i)}{d_{in}}\} \le \frac{2\Delta(y_i,w_i)}{d_{in}} = \frac{2\Delta(y_i,c_i)}{d_{in}} = \frac{2\cdot e_i}{d_{in}}$

$\Rightarrow \mathbb{E}\left[Z_i^{erasure} + 2Z_i^{error}\right] \le \frac{2e_i}{d_{in}}$.

Случай 2 $w_i \ne c_i$

$\mathbb{E}\left[Z_i^{erasure}\right] = \min\{1, \frac{2\Delta(y_i,w_i)}{d_{in}}\} = \frac{2}{d_{in}} \min\{\frac{d_{in}}{2}, \Delta(y_i,w_i)\}$

$Z_i^{error} = 1 - Z_i^{erasure}$ (по определению)

$\mathbb{E}\left[Z_i^{error}\right] = 1 - \mathbb{E}\left[Z_i^{erasure}\right]$

$\mathbb{E}\left[2\cdot Z_i^{error} + Z_i^{erasure}\right] = 2\cdot(1 - \mathbb{E}[Z_i^{erasure}]) + \mathbb{E}[Z_i^{erasure}]$

$= 2 - \mathbb{E}\left[Z_i^{erasure}\right] = 2 - \frac{2}{d_{in}} \min\{\frac{d_{in}}{2}, \Delta(y_i,w_i)\}$.

т.к. $w_i \ne c_i$, имеем

$d_{in} \underset{(\text{т.к. } c_i, w_i \in C_{in})}{\le} \Delta(c_i, w_i) \underset{(\text{н-во } \Delta\text{-ка})}{\le} \Delta(c_i, y_i) + \Delta(y_i, w_i) = e_i + \Delta(y_i, w_i)$

$$\Rightarrow d_{in} \leq e_i + \Delta(y_{i_i}, w_i) \Rightarrow \Delta(y_{i_i} w_i) \geq d_{in} - e_i$$

1) $\min\{\} = \Delta(y_{i_i}, w_i)$. Тогда

$$2 - \frac{2}{d_{in}} \cdot \Delta(y_{i_i} w_i) \leq 2 - \frac{2}{d_{in}}(d_{in} - e_i) = 2 - 2 + \frac{2e_i}{d} = \frac{2e_i}{d_{in}}$$

2) $\min\{\} = \frac{d_{in}}{2}$. Тогда из н-ва

$$\left.\begin{array}{l} e_i + \Delta(y_{i_i} w_i) \geq d_{in} \\ \min\{\} = \frac{d_{in}}{2} \end{array}\right\} \Rightarrow \min \geq d_{in} - e_i$$

$$\Rightarrow 2 - \frac{2}{d_{in}} \cdot \min\{\} \leq 2 - \frac{2(d_{in} - e_i)}{d_{in}} = \frac{2e}{d_{in}} \quad \blacksquare$$

Замечание: Алгоритм можно сделать детерминированным, обозначив в начале алг-ма границу в-ти (Ω).