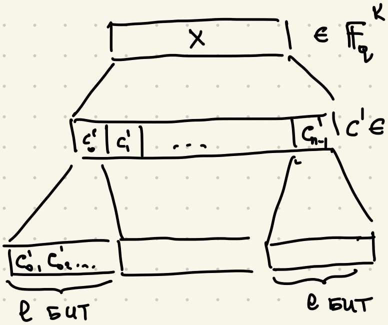
Лекция №11

Коды конкатенации

Идея



$\mathbb{F}_q = \mathbb{F}_2^l$

Код конкатенации: положим $C_{out} \subseteq \mathbb{F}_{q_{out}}^{n_{out}}$ – $[n_{out}, k_{out}, d_{out}]$ – внешний лин. код

$C_{in} \subseteq F_{q_{in}}^{n_{in}}$ – $[n_{in}, k_{in}, d_{in}]$ – внутр. лин. код $\quad q_{out} = q_{in}^{k_{in}}$

Код конкатенации $C_{in} \circ C_{out} \subseteq \mathbb{F}_{q_{in}}^{n_{out} \cdot n_{in}}$ – это лин. код с ф-цией кодирования Enc $x \in \mathbb{F}_{q_{in}}^{k_{in} \cdot k_{out}}$, заданной след. образом:

1. $x \in \left(\mathbb{F}_{q_{in}}^{k_{in}}\right)^{k_{out}} \cong \left(\mathbb{F}_{q_{out}}\right)^{k_{out}}$

2. кодируем x с помощью $Enc_{out}(x) \to c' \in \mathbb{F}_{q_{out}}^{n_{out}} = \left(\mathbb{F}_{q_{in}}\right)^{k_{in} \cdot n_{out}}$

3. кодируем $\forall\ c'_i$, $i \leq n_{out}$ с помощью $Enc_{in}()$,

$$c = Enc_{in}(c'_1) \,\|\, Enc_{in}(c'_2) \ldots \|\, Enc(c'_{n_{out}})$$

Пар-ры кода:

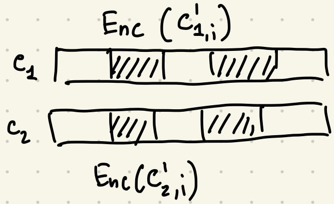
1) размерность: $k_{in} \cdot k_{out} =: k$ $\Rightarrow$ скорость: $R = \frac{k}{n} = R_{out} \cdot R_{in}$

2) длина: $n_{in} \cdot n_{out} =: n$

Предложение 1

Min. расстояние $C_{in}\circ C_{out} \geq d_{in}\cdot d_{out}$

◁ $\exists\ c_1, c_2 \in C_{in}\circ C_{out}$



1) как min. d_{out} блоков c_1, c_2 кодируют разные символы $\mathbb{F}_{q_{in}}$

2) каждый эл-т одного из таких блоков кодируется в слово из C_{in} с min. расстоянием d_{in}

$\Rightarrow$ всего как min. $d_{out}\cdot d_{in}$ отличий c_1 от c_2. ▷

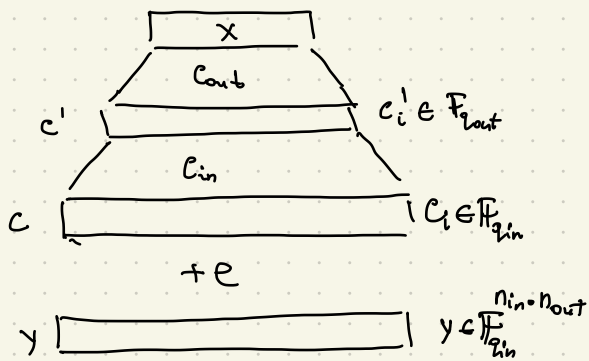
Пример

1. C_{out} – код Рида-Соломона
2. C_{in} – асимптот. хороший бинарный код (код порождённый случ. матрицей $G\in\mathbb{F}_2^{k\times n}$)

II Декодирование $C_{in}\circ C_{out}$

Попытка №1

Алгоритм #1



1) декодировать каждое $y_i \in \mathbb{F}_{q_{in}}^{n_{in}}$ с помощью декодера C_{in}:

$$w_i' = \underset{c\in C_{in}}{\arg\min}\, \Delta(y_i, c) \in \mathbb{F}_{q_{in}}^{n_{in}}$$

2) получить соответствующее сообщение m_i' т.ч. $w_i' = Enc_{in}(m_i')$
$\in \mathbb{F}_{q_{in}}^{k_{in}} = \mathbb{F}_{q_{out}}$

3) декодировать $(m_1', .., m_{n_{out}}')$ с помощью декодера C_{out}.

Лемма №1 Алг-м #1 может декодировать $< \frac{d_{in} \cdot d_{out}}{4}$ ошибок

(Замечание: "хороший" алг-м декодирования для $C_{in} \circ C_{out}$ должен декодировать $\left\lfloor \frac{d_{in} \cdot d_{out} - 1}{2} \right\rfloor$ ошибок)

◁ Назовём блок $y_i \in \mathbb{F}_{q_{in}}^{n_{in}}$ "плохим", если в нём больше, чем $\left\lfloor \frac{d_{in} - 1}{2} \right\rfloor$ ошибок.

Т.к. у нас всего $wt(e)$ ошибок, то максимум $\frac{wt(e)}{\left\lfloor \frac{d_{in}-1}{2} \right\rfloor}$ блоков "плохие". Декодер C_{in} не может декодировать такие y_i на шаге 1. $\Rightarrow$ В этом случае, Dec_{out} получит на вход слово $\notin C_{out}$. Число таких слов $\leq \left\lfloor \frac{d_{out}-1}{2} \right\rfloor$

В итоге, # "плохих" блоков $\leq \left\lfloor \frac{d_{out}-1}{2} \right\rfloor$

$$\frac{wt(e)}{\left\lfloor \frac{d_{in}-1}{2} \right\rfloor} \leq \left\lfloor \frac{d_{out}-1}{2} \right\rfloor \Rightarrow wt(e) \leq \left\lfloor \frac{d_{in}-1}{2} \right\rfloor \cdot \left\lfloor \frac{d_{out}-1}{2} \right\rfloor < \frac{d_{in} d_{out}-1}{4}$$ ▶

Попытка №2

Замечание Когда мы декодируем y_i на шаге 1, получаем помимо $w_i' \in C_{in}$, расстояние $\Delta(y_i, w_i')$. Суть алг-ма 2: каждому w_i' приписывается "уровень доверия" (confidence level), зависящий от $\Delta(y_i, w_i')$)

В случае, если $\Delta(y_i, w_i')$ большое, считаем y_i – удалённым символом "*".

Лемма (возможности декодир-ия кода Рида-Соломона) Мы можем декодировать $RS_{\mathbb{F}_q, \mathbb{F}_q^*}(n, k)$ с $wt(e)$ ошибками и s удалёнными символами, если $2wt(e) + s < n - k + 1$.

Алгоритм №2 (Форней)

Вход: $y = (y_1 \dots y_{n_{out}}) \in \left(\mathbb{F}_{q_{in}}^{n_{in}}\right)^{n_{out}}$

1. Для $i = 1 \dots n_{out}$:

   1.1. $w_i = \underset{c \in C_{in}}{\operatorname{argmin}}\, \Delta(y_i, c) \in \mathbb{F}_{q_{in}}^{n_{in}}$

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

   $w_i = "*"$

   иначе

   m_i' — т.ч. $Enc_{in}(m_i') = w_i$

2. $X = Decode_{out}(m_1' \dots m_{n_{out}}')$

Лемма 2 $\mathbb{E}\left[\,|w_i| = "*" + 2|w_i \notin C_{out}|\,\right] < d_{out}$

("декодирование на шаге 2 Алг-ма №2 пройдёт успешно "в среднем" ")

$\triangleleft$ $e_i := \Delta(y_i, c_i)$

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

Обозначим для $i \le n_{out}$: $Z_i^{erasure} = \begin{cases} 1, & w_i = "*" \\ 0, & \text{иначе} \end{cases}$, $Z_i^{error} = \begin{cases} 1, & w_i \neq "*", c_i \neq C_{out} \\ 0, & \text{иначе} \end{cases}$

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

{ из (1) $\Rightarrow$ утверждение леммы 2, т.к. $\mathbb{E}\left[\sum_{i \le n_{out}} Z_i^{erasure} + 2\sum_{i \le n_{out}} Z_i^{error}\right]$
$= \sum_{i \le n_{out}} \mathbb{E}\left[Z_i^{erasure} + 2Z_i^{error}\right] \overset{(1)}{\le} \sum_{i \le n_{out}} \dfrac{2e_i}{d_{in}} < \dfrac{\cancel{2}}{\cancel{d_{in}}} \cdot \dfrac{\cancel{d_{in}} \cdot d_{out}}{\cancel{2}} = d_{out}$ }

СЛУЧАЙ №1 $\quad \underline{w_i = c_i}$

$$z^{error} = 0$$

$$\mathbb{E}[z^{erasure}] = 1 \cdot \Pr[w_i = \text{"}*\text{"}] + 0 \cdot \Pr[w_i \neq \text{"}*\text{"}]$$

$$= \min\left(1, \frac{2\Delta(y_i, w_i)}{d_{in}}\right) \leq \frac{2\Delta(y_i, w_i)}{d_{in}} = \frac{2\Delta(y_i, c_i)}{d_{in}}$$

$$= \frac{2e_i}{d_{in}} \Rightarrow \mathbb{E}[2z_i^{error} + z_i^{erasure}] \leq \frac{2e_i}{d_{in}}.$$

СЛУЧАЙ №2 $\quad w_i \neq c_i$

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

$$z^{error} = 1 - z^{erasure} \text{ (по определению)}$$

$$\mathbb{E}[z^{error}] = \mathbb{E}[1 - z^{erasure}] = 1 - \mathbb{E}[z^{erasure}] \Rightarrow$$

$$\mathbb{E}[2z^{error} + z^{erasure}] = 2(1 - \mathbb{E}[z^{erasure}]) + \mathbb{E}[z^{erasure}]$$

$$= 2 - \mathbb{E}[z^{erasure}]$$

$\Big\{$ т.к. $w_i \neq c_i$, имеем $d_{in} \leq (c_i, w_i) \leq \Delta(c_i, y_i) + \Delta(y_i, w_i)$

(т.к. $c_i, w_i \in C_{in}$) $\quad$ н-во Δ-ка

$= e_i + \Delta(y_i, w_i)$ $\Big\}$

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

$\min = \Delta(y_i, w_i)$

$$2 - \frac{2}{d_{in}} \Delta(y_i, w_i) = 2\left(1 - \frac{1}{d_{in}} \Delta(y_i, w_i)\right)$$

$$\leq 2\left(1 - \frac{d_{in} - e_i}{d_{in}}\right) = 2\left(1 - 1 + \frac{e_i}{d_{in}}\right) = \frac{2e_i}{d_{in}}$$

$\min = \frac{d_{in}}{2}$

$e_i \geq \frac{d_{in}}{2}$ (иначе, внутр. декодер сработал бы корректно)

$$\frac{d_{in}}{2} + e_i \geq d_{in}$$

$$\min\{\} + e_i \geq d_{in} \Rightarrow \min\{\} \geq d_{in} - e_i \Rightarrow$$

$$\Rightarrow 2 - \frac{2}{d_{in}} \min\{\} \leq$$

$$2 - \frac{2}{d_{in}}\left(d_{in} - e_i\right) = 2 - 2 + \frac{2e_i}{d_{in}} =$$

$$= \frac{2e_i}{d_{in}}$$