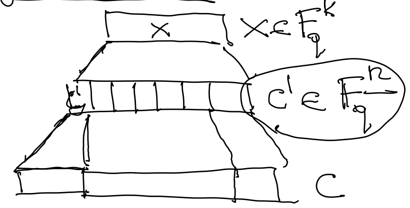
Идея: каждый символ $\mathbb{F}_q \to \lg(q)$ бит $\Rightarrow$ бинарный код.



I. Параметры кода конкатенации

Опр-ие Положим, $C_{out} \subseteq \mathbb{F}_{q_{out}}^{n_{out}}$ – $[n_{out}, k_{out}, d_{out}]$ – внешний лин. код

$C_{in} \subseteq \mathbb{F}_{q_{out}}^{n_{in}}$ – $[n_{in}, k_{in}, d_{in}]$ – внутр. лин. код,

$\mathbb{F}_{q_{out}} \cong (\mathbb{F}_{q_{in}})^{k_{in}}$,

$q_{out} = q_{in}^{k}$

$(q_{in} = 2)$

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

1) рассматр. $x \in (\mathbb{F}_{q_{in}}^{k_{in}})^{k_{out}} \simeq (\mathbb{F}_{q_{out}})^{k_{out}}$

2) кодируем x с помощью $Enc_{out}(x) \to C' \in \mathbb{F}_{q_{out}}^{n_{out}}$ $\cong (\mathbb{F}_{q_{in}})^{k_{in} n_{out}}$

3) кодируем C'_i, $i = \overline{1, n_{out}}$ с помощью внутр. $Enc_{in}()$:

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

конкатенация

$Enc_{in}: \mathbb{F}_{q_{in}}^{k_{in}} \to \mathbb{F}_{q_{in}}^{n_{in}}$.

Пар-ры кода конкатенации:

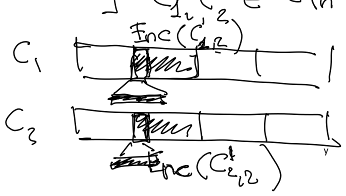
1) р-ть кода $k = k_{in} \cdot k_{out}$

2) длина кода $n = n_{in} \cdot n_{out}$

$\Rightarrow R = \frac{k}{n} = R_{in} \cdot R_{out}$

Предложение 1 Min. расстояние $C_{in} \circ C_{out} \geq d_{in} \cdot d_{out}$

$\triangle$ Пусть $c_1, c_2 \in C_{in} \circ C_{out}$, $c_1 \neq c_2$



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

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

$\Rightarrow$

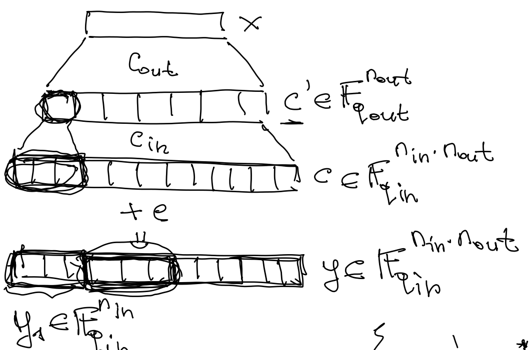
$\Rightarrow$ всего как min. $d_{in} \cdot d_{out}$ разных символов над $\mathbb{F}_{q_{in}}$. $\blacksquare$

Пример . C_{out} – код Рида-Соломона

. C_{in} – асимптотически "хороший" бинарный код (код, порождённый случайной 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}, а именно

$$w_i' = \underset{c \in C_{in}}{\operatorname{argmin}}\, \Delta(y_i, c),$$

$w_i' \in \mathbb{F}_{q_{in}}^{n_{in}}$

2) Получить соотв. сообщение m_i' т.ч. $w_i' = Enc_{in}(m_i')$ $\{ w_i' = m_i' \cdot G_{in} \}$

3) Декодировать $(m_1', \dots, m_{n_{out}}') \in \mathbb{F}_{q_{out}}^{n_{out}}$

Лемма 1 Алгоритм №1 может декодировать $< \dfrac{d_{in} \cdot d_{out}}{4}$ ошибок

$\boxed{\text{Замечание}}$ хороший алг-м для $C_{in} \cdot C_{out}$ должен декодировать $\left\lfloor \dfrac{d_{in} \cdot d_{out} - 1}{2} \right\rfloor$ ошибок

Д Назовём блок $y_i \in \mathbb{F}_{q_{in}}^{n_{in}}$ - "плохим", если в нём больше, чем $\left\lfloor \dfrac{d_{in} - 1}{2} \right\rfloor$ ошибок. Т.к. всего у нас $wt(e)$ ошибок, то максимум $\dfrac{wt(e)}{\left\lfloor \frac{d_{in}-1}{2} \right\rfloor}$ блоков y_i "плохие". (декодер для C_{in} не может корректно декодировать такие y_i)

В этом случае алг-м декодирования для C_{out} получит на вход слово $\notin C_{out}$. Число таких слов $\le \left\lfloor \dfrac{d_{out} - 1}{2} \right\rfloor$. В итоге,

$$\#\text{плохих блоков} \le \left\lfloor \frac{d_{out} - 1}{2} \right\rfloor$$

$$\frac{wt(e)}{\left\lfloor \frac{d_{in}-1}{2} \right\rfloor} \le \left\lfloor \frac{d_{out} - 1}{2} \right\rfloor \Rightarrow wt(e) \le \left\lfloor \frac{d_{in}-1}{2} \right\rfloor \cdot \left\lfloor \frac{d_{out}-1}{2} \right\rfloor \approx \frac{d_{in} \cdot d_{out}}{4} \quad \blacksquare$$

Попытка №2

Замечание: Когда мы декодируем y_i, мы получаем помимо $w_i' \in C_{in}$, расстояние $\Delta(y_i, w_i')$. Суть Алгоритма 2: каждому w_i' приписывается "уровень доверия" (confidence measure), зависящий от $\Delta(y_i, w_i')$. В случае, если $\Delta(y_i, w_i')$ превышает заданную границу, считаем y_i - удалённым ("$*$").

Случай 1 Блок y_i имеет $> \left\lfloor \dfrac{d_{in}-1}{2} \right\rfloor$ ошибок, но $< d_{in}$ $\Rightarrow$ декодирование на шаге 1 Алг-ма 1 не будет успешным (w_i' не будет найдено). Этот случай мы можем детектировать, считаем y_i удалённым символом;

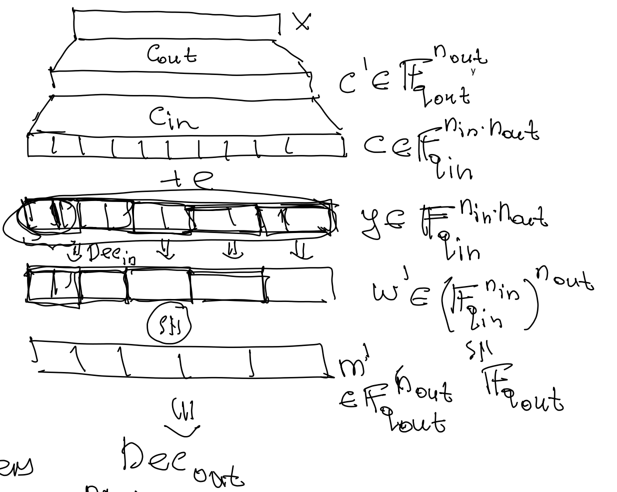
Случай 2 В $y_i \ge d_{in}$ ошибок $\Rightarrow y_i$ декодируется к $\tilde{w}_i' \in C_{in}$, где $\tilde{w}_i'$ не является исходным кодовым словом для y_i. Таких блоков $< \dfrac{wt(e)}{d_{in}}$; Полагаем, что такой случай встречается с малой вероятностью случаи встречаются с малой вероятностью.

Лемма 2 Мы можем эффективно декодировать $RS_{\mathbb{F}_q, \mathbb{F}_q^*}(n,k)$ с $wt(e)$ ошибками и с S удалёнными символами, если

$$\underbrace{2wt(e)} + \underbrace{S} < \underbrace{n-k+1}_{d(RS)}.$$

◁ Док-во дома ▷.

Алгоритм №2 (вероятностный) Алгоритм Форней (Forney) / Обобщённый алг-м декодир. с min. расстоянием



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

1. для $i = 1 \dots n_{out}$

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

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

   $m_i' =$ "*"

   иначе

   $m_i' = w_i'$ (при этом полагаем $m_i' \in \mathbb{F}_{q_{out}} \cong \mathbb{F}_{q_{in}}^{n_{in}}$)

2. $c' = Decode_{C_{out}}(m_1', \dots, m_{out}')$

Вернуть c'.

Сложность алг-ма 2: $\boxed{n_{out} \cdot Time(Decode_{C_{in}}) + Time(Decode_{C_{out}})}$

Если C_{out} берём RS, $Time(Decode_{RS}) = poly(n_{out})$

C_{in} берём случайный $[n_{in}, k_{in}, d_{in}]$-лин. код над $\mathbb{F}_2$,

$Time(Decode_{out}) = 2^{O(n_{in})}$ ⇒ n_{in} должно быть мало;

Корректность алг-ма 2

Предложение

$$\mathbb{E}_{\substack{(\text{случ. алг-ма 2} \\ \text{на шаге 1.2})}} \left[|m_i' = \text{"*"}| + 2|m_i' \notin C_{out}| \right] < d_{out}$$

т.е. условие леммы 2 выполняется "в среднем".

Док-во на след. лекции;