Лекция 7

Ilya Yaroshevskiy

20 октября

Содержание

1 Функция переходных вероятностей канала

Канал без памяти с входныи алфавитом

Определение. $W(y|c)$ – вероятность наблюдения на выходе канала $y \in \mathcal{Y}$ при условии подачи на его вход $c \in \mathcal{X}$

Пример. Двоичный симметричный канал: $\mathcal{Y} = \mathcal{X}, W(y|c) = \begin{cases} p & , y \neq x \\ 1-p & , y = x \end{cases}$

Пример. Двоичный стирающий канал $\mathcal{Y} = \{0, 1, \varepsilon\}$: $W(y|c) = \begin{cases} p & , y = \varepsilon \\ 1-p & , y = x \in \{0, 1\} \end{cases}$

Пример. Двоичный симметричный канал со стираниями $\mathcal{Y} = \{0, 1, \varepsilon, W(y|c) = \begin{cases} 1-p-s & , y = x \\ s & , y = \varepsilon \\ p & , y = 1-x \end{cases}$

Непрервыный выходной алфавит $\mathcal{Y}$. $W(y|c)$ – плотность распределения выходного символа канала при подаче c на его вход. Аддитивный науссовский канал:
$\mathcal{Y} = \mathbb{R}, y = (-1)^c + \eta, \eta \sim \mathcal{N}(0, \sigma^2), W(y|c) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{|y-(-1)^c|^2}{2\sigma^2}}$ Для простоты, будем считать $\mathcal{Y}$ дискретным

2 Параметр Бхаттачарьи

Определение. Рассмотрим приемник по максимуму прадоподобия $\tilde{c} = \text{argmax}_{c\in 0,1} W(y|c)$. Передаваемые символы рановероятны. Вероятность ошибки

$$\begin{aligned}
P_c &= P\{c=0\}P\{err|e=0\} + P\{c=1\}P\{err|c=1\} = \\
&= \frac{1}{2}\sum_{y:W(y|0)<W(y|1)} W(y|0) + \frac{1}{2}\sum_{y:W(y|1)<W(y|0)} W(y|1) = \\
&= \frac{1}{2}\sum_{y:\frac{W(y|1)}{W(y|0)}>1} W(y|0) + \frac{1}{2}\sum_{y:\frac{W(y|0)}{W(y|1)}>1} W(y|1) = \\
&= \frac{1}{2}\sum_{y\in\mathcal{Y}}\sum_{c\in\{0,1\}}\left(W(y|c)\chi\left(\frac{W(y|1-c)}{W(y|c)}\right)\right)
\end{aligned}$$

Индикаторная фунукция $\chi(z) = \begin{cases} 1 & ,z \geq 1 \\ 0 & ,z < 1 \end{cases}$

$$P_c \leq \frac{1}{2}\sum_{y\in\mathcal{Y}}\sum_{c\in\{0,1\}}\left(W(y|c)\chi\left(\frac{W(y|1-c)}{W(y|c)}\right)\right) = \sum_{y\in\mathcal{Y}}\sqrt{W(y|0)W(y|1)} = Z(W)$$

Пример. Двоичный стирающий канал

$$Z(BEC(p)) = \sqrt{W(0|0)W(0|1)} + \sqrt{W(1|0)W(1|1)} + \sqrt{W(\varepsilon|0)W(\varepsilon|1)} = p$$

Пример. Аддитивный гауссовский канал:

$$Z(\mathcal{G}(\sigma)) = \int_{-\infty}^{\infty}\sqrt{W(y|0)W(y|1)}dy = \frac{1}{\sqrt{2\pi\sigma^2}}\int_{-\infty}^{\infty} e^{-\frac{(y-1)^2+(y+1)^2}{2\sigma^2}}dy = \frac{e^{-\frac{1}{2\sigma^2}}}{\sqrt{2\pi\sigma^2}}\int_{-\infty}^{\infty} e^{-\frac{y^2}{2\sigma^2}}dy = e^{-\frac{1}{2\sigma^2}}$$

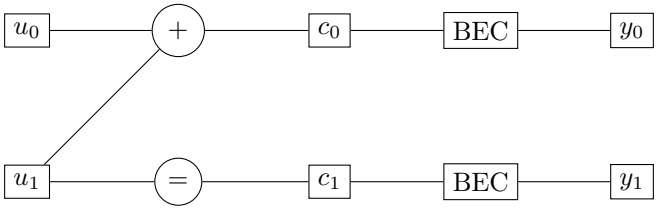
3 Пропускная способность канала

$$I(W) = \max_{\{p(x)\}}\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} W(y|x)P\{x\}\log\frac{W(y|x)}{W(y)}$$

Сущесутвуют методы сколь угодно надежной передачи данных со скоростью $R < I(W)$. При передаче данных со скоростью $R > I(W)$ вероятность ошибки ограничена снизу положительной величиной. Для многих каналов оптимальным распределением символов на входе $P\{x\}$ является равномерное

4 Поляризация канала

Определение. Рассмотрим линейное преобразование, задаваемое



$$\begin{pmatrix} c_0 & c_1 \end{pmatrix} = \begin{pmatrix} u_0 & u_1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Двоичный стирающий канал: $y = \begin{cases} c_i & ,\text{с вероятностью } 1-p \\ e & ,\text{с вероятностью } p \end{cases}$

- u_0 не может быть восстановлен из y_0, y_1 с вероятностью $1-(1-p)^2 = 2p-p^2 \geq p$
- u_1 не может быть восстановлен из u_0, y_0, y_1 с вероятностью $p^2 \leq p$

5 Битовые подканалы

Пусть $A_m = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes m}$, где $\otimes m$ обозначает m-кратное произведение Кронекерра матрицы с собой. Пусть $n = 2^m$.

Определение. Краткая запись подвекторов $y_a^b = (y_a, y_{a+1}, \dots, y_b)$

$$W_m(y_0^{n-1}|c_0^{n-1}) = \prod_{i_0}^{n-1} W(y_i|c_i)$$

Синтетические битовые подканалы

$$W_m^{(i)}(y_0^{n-1}, u_0^{i-1}|u_i) = \frac{W_m^{(i)}(y_0^{n-1}, u_0^i)}{P\{u_i\}} = 2 \sum_{u_{i+1}^{n-1} \in \mathbb{F}_2^{n-1}} W_m^{(n-1)}(y_0^{n-1}|u_0^{n-1}) P\{u_0^{n-1}\} =$$

$$= \frac{2}{2} \sum_{?} W_m(y_0^{n-1}|u_0^{n-1} A_m) = 2^{-n+1} \sum_{?} \prod_{?}^{n-1} W(y_j|(u_0^{n-1} A_m))$$ Исправить

6 Функция переходных вероятностей битовых подканалов

$$W_1^{(0)}(y_0, y_1|u_0) = \frac{1}{2} \sum_{u_1=0}^{1} W(y_0|u_0 + u_1) W(y_1|u_1)$$

$$W_1(y_0, y_1, u_0|u_1) = \frac{1}{2} W(y_0|u_0 + u_1) W(y_1|u_1)$$

7 Рекурсивное определение подканалов

$$W_\lambda^{2i}(y^{2^\lambda - 1}, u_0^{2i-1}|u_{2i}) = \frac{1}{2} \sum_{u_{2i+1}=0}^{1} W_{\lambda-1}^{(i)}(y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1} + u_{0,\text{odd}}^{2i-1}|u_{2i} + u_{2i+1}) W_{\lambda-1}^{(i)}(y_{0,\text{odd}}^{2^\lambda-1}, u_{0,\text{odd}}^{2i-1}|u_{2i+1})$$

$$\mathrm{W}_\lambda^{(2i+1)}(y_0^{2^\lambda-1}, u_0^{2i}|u_{2i+1}) = \tfrac{1}{2} W_{\lambda-1}^{(i)}(y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1} + u_{0,\text{odd}}^{2i-1}|u_{2i} + u_{2i+1}) W_{\lambda-1}^{(i)}(y_{0,\text{odd}}^{2^\lambda-1}, u_{0,\text{odd}}^{2i-1}|u_{2i+1})$$

Доделать Картинка ez

8 Параметры подканалов

Определение. Параметры Бхаттачарьи битовых подканалов $Z_{m,i} = Z(W_m^{(i)})$

$$Z_{m,2i+1} \leq Zm, 2i \leq 2Z_{m-1,i} - Z_{m-1,i}^2$$

$$Z_{m,2i+1} = Z_{m-1,i}^2$$

Строгое равенство в случае двоичного стирающего канала

Замечание. Пропускные способности битовых подканалов $I_{m,i} = I(W_m^{(i)})$

$$I_{m,2i} + I_{m,2i+1} = 2I_{m-1,i}$$

$$I_{m,2i} \leq I_{m,2i+1}$$

$$\sqrt{1 - Z(W)^2} \geq I(W) \geq \log \frac{2}{1 + Z(W)}$$

Для любого $\delta \in (0, 1)$ при $m \to \infty$ доля подканалов с $I(W_m^{(i)}) \in (1 - \delta, 1]$ стермиться к $I(W_0^{(0)}) - I(W)$, а доля подканалов с $I(W_m^{(i)}) \in [0, \delta)$ стремится к $1 - I(W)$

Замечание. Поляризация каналов: Доделать Картинка

- Доля недополяризованных подканалов убывает с увеличением m
- Число недополяризованных подканалов растет с увеличением m

9 Полярный код и алгоритм последовательного исключения

Замечание. Передавать предопределенные значения (например, 0) по плохим подканалам. Кодирование $c_0^{n-1} = u_0^{n-1} A_m, u_i = 0, i \in \mathcal{F}$, где $\mathcal{F}$ – множество номеров плохих подканалов (замороженных символов). Линейный блоковый код $(2^m, 2^m + |\mathcal{F}|)$

Program 1 Алгоритм последовательного исключения

1: **for** $i = 0, 1, \ldots, 2^m - 1$ **do**

2: $\hat{u}_i = \begin{cases} 0 & , i \in \mathcal{F} \\ \operatorname{argmax}_{u_i} W_m^{(i)}(y_0^{n-1}, \hat{u}_0^{i-1} | u_i) & , i \notin \mathcal{F} \end{cases}$

3: **end for**

- Если предыдущие решения были правильными, то $\hat{u}_0^{i-1} = u_0^{i-1}$

Если ранее была допущена ошибка, алгоритм ПИ все равно не сможет ее исправить. Вероятность ошибки $P \leq \sum_{i \notin \mathcal{F}} Z_{m,i} \leq 2^{-n^\beta}, \beta < 0.5$

9.1 Сложность кодирования

$$u_0^{n-1} A_m = \begin{pmatrix} u_0^{n/2-1} & u_{n/2}^{n-1} \end{pmatrix} \begin{pmatrix} A_{m-1} & 0 \\ A_{m-1} & A_{m-1} \end{pmatrix} = \begin{pmatrix} (u_0^{n/2-1} + u_{n/2}^{n-1}) A_{m-1} & u_{n/2}^{n-1} A_{m-1} \end{pmatrix}$$

Сложность $T(n) = 2T(n/2) + n/2 = \frac{1}{2} n \log_2 n$

9.2 Декодер с ЛОПП

Логарифмическое отношение правдоподобия $L_m^{(i)}(y_0^{n-1}, u_0^{i-1}) = \ln \frac{W_m^{(i)}(y_0^{n-1}, u_0^{i-1}|0)}{W_m^{(i)}(y_0^{n-1}, u_0^{i-1}|1)}$

$$L_\lambda^{2i+1}(y_0^{n-1}, u_0^{i-1}) = \log \frac{W_{\lambda-1}^{(i)}(y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1} + u_{0,\text{odd}}^{2i-1} | u_{2i} + 0) W_{\lambda-1}^{(i)}(y_{0,\text{odd}}^{2^\lambda-1}, u_{0,\text{odd}}^{2i-1} | 0)}{W_{\lambda-1}^{(i)}(y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1} + u_{0,\text{odd}}^{2i-1} | u_{2i} + 1) W_{\lambda-1}^{(i)}(y_{0,\text{odd}}^{2^\lambda-1}, u_{0,\text{odd}}^{2i-1} | 1)} =$$
$$= (-1)^{u_{2i}} L_{\lambda-1}(y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1} + u_{0,\text{odd}}^{2i-1}) + L_{\lambda-1}(y_{0,\text{odd}}^{2^\lambda-1}, u_{0,\text{odd}}^{2i-1})$$

Пусть

$$p_s = W_\lambda^{(2i)}(s | y_0^{2^\lambda-1}, u_0^{2i-1}) = \frac{W_\lambda^{(2i)}(y_0^{2^\lambda-1}, u_0^{2i-1} | s) P\{u_{2i} = s\}}{W_\lambda^{(2i)}(y_0^{2^\lambda-1}, u_0^{2i-1})} = \frac{W_\lambda^{(2i)}(y_0^{2^\lambda-1}, u_0^{2i-1} | s)}{2 W_\lambda^{(2i)}(y_0^{2^\lambda-1}, u_0^{2i-1})}$$

$$p_{0s} = W_{\lambda-1}^{(i)}(s | y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1} + u_{0,\text{odd}}^{2i-1})$$

$$p_{1s} = W_{\lambda-1}^{(i)}(s | y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1}), s \in \{0, 1\}$$

$$p_0 = p_{00} p_{10} + p_{01} p_{11}$$

$$p_1 = p_{01} p_{10} + p_{00} p_{11}$$

$$p_0 + p_1 = 1, p_{i0} + p_{i1} = 1, i \in \{0, 1\}$$

$$\tanh\left(\frac{1}{2} \ln \frac{p_0}{p_1}\right) = \frac{\exp(\ln(p_0/p_1)) - 1}{\exp(\ln(p_0/p_1)) + 1} = p_0 - p_1 = 1 - 2p_1$$

$$1 - 2p_1 = (1 - 2p_{01})(1 - 2p_{11}) = 1 - 2(p_{01} + p_{11} - 2p_{11}p_{01}) = 1 - 1(p_0(1 - p_{11}) + (1 - p_{01})p_{11})$$

$$\tanh\left(\frac{1}{2} L_\lambda^{(2i)}(y_0^{n-1}, u_0^{2i-1})\right) = \tanh\left(\frac{1}{2} L_{\lambda-1}^{(i)}(y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1} - u_{0,\text{odd}}^{2i-1})\right) \tanh\left(\frac{1}{2} L_{\lambda-1}^{(i)}(y_{0,\text{odd}}^{2^\lambda-1}, u_{0,\text{odd}}^{2i-1})\right)$$

$$L_\lambda^{(2i)}(y_0^{2^\lambda-1}, u_0^{2i-1}) = 2 \tanh^{-1}\left(\tanh\left(\frac{1}{2} L_{\lambda-1}^{(i)}(y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1} + u_{0,\text{odd}}^{2i-1})\right) \tanh\left(\frac{1}{2} L_{\lambda-1}^{(i)}(y_{0,\text{odd}}^{2^\lambda-1}, u_{0,\text{odd}}^{2i-1})\right)\right)$$

$$L_\lambda^{(2i+1)}(y_0^{n-1}, u_0^{2i}) = (-1)^{u_{2i}} L_{\lambda-1}(y_{0,\text{even}}^{2^\lambda-1}, u_{0,\text{even}}^{2i-1} + u_{0,\text{odd}}^{2i-1}) + L_{\lambda-1}(y_{0,\text{odd}}^{2^\lambda-1}, u_{0,\text{odd}}^{2i-1})$$

Program 2 Алгоритм последовательного исключения с ЛОПП

1: **for** $i = 0, 1, \ldots, 2^m$ **do**

2: $$\hat{u}_i = \begin{cases} 0 & , i \in \mathcal{F} \\ 0 & , L_m^{(i)}(y_0^{n-1}, \hat{u}_0^{i-1}) > 0, i \notin \mathcal{F} \\ 1 & , L_m^{(i)}(y_0^{n-1}, \hat{u}_0^{i-1}) \le 0, i \notin \mathcal{F} \end{cases}$$

3: **end for**

9.3 Другой вариант алгоритма последовательного исключения

$$W_m^{(i)}(u_0^i | y_0^{n-1} d$$

$$2\mathrm{W}(\mathrm{y}_0^{n-1}) = \omega \sum_{u_{i+1}^{n-1}} \prod_{j=0}^{n-1} W((u_0^{n-1} A_m)|y_j)$$

$$W_\lambda^{(2i)}(u_0^{2i}|y_0^{n-1}) = \omega \sum_{u_{2i+1}} W_{\lambda-1}^{(i)}(u_{2t} + u_{2t+1}, 0 \le t \le i | y_{0,\mathrm{even}^{n-1}}) W_{\lambda-1}(u_{2t+1}, 0 \le t \le i | y_{0,\mathrm{odd}}^{n-1})$$

$$W_\lambda^{(2i+1)}(u_0^{2i-1}|y_0^{n-1}) = \omega W_{\lambda-1}^{(i)}(u_{2t} + u_{2t+1}, 0 \le t \le i | y_{0,\mathrm{even}^{n-1}}) W_{\lambda-1}(u_{2t+1}, 0 \le t \le i | y_{0,\mathrm{odd}}^{n-1})$$

Доделать Картинка: зеленый – принятый вектор

Переиспользование на фазе $2i+1$ сомножителей $W_{\mu-1}^{(i)}$, вычисленных на фазе $2i$. При обновлени на слое λ вычисляют $2^{m-\lambda}$ ЛОПП. Сложность $C = \sum_{\lambda=1}^{m} 2^\lambda \cdot 2^{m-\lambda} = m2^m = n \log_2 n$. Сложность $O(n \log_2 n)$. Размер памяти $O(n)$.

9.4 Построение $(2^m, k)$ полярного кода

Замораживанию подлежат $2^m - k$ наименее надежных символов (например, с наибольшим $Z_{m,i}$. Двоичный стирающий канал

$$Z_{m,2i} = 2Z_{m-1,i} - Z_{m-1,i}^2$$
$$Z_{m,2i+1} = Z_{m-1,i}^2$$

Сложность вычисления $Z_{m,i} = O(n)$. В общем случае выходной алфавит канала $W_m^{(i)}(y_0^{n-1}, u_0^{i-1}|u_i)$ имеет мощность $|\mathcal{Y}|^n 2^i$. Построение функции переходных вероятностей $W_m^{(i)}$ вычислительно нереализуемо уже при небольших m. Можно аппроксимировать канал $W_m^{(i)}$ каналом с выходным алфавитом фиксированной мощности μ, который был бы чуть лучше или чуть хуже, чем истинный $W_m^{(i)}$. $Z_{m,i}$ могут быть вычисленны со сложностью $O(n\mu^2 \log \mu)$.

9.5 Гауссовская аппроксимация

Полярные коды являются линейными. Для симметричных канало вероятность ошибки не зависит от того, какое кодовое слова передавалось. Будем считать, что передавалось 0 слово. Рассмотрим передачу кодовых слов по аддитивному гауссовскому каналу:
$y_i = (-1)^{c_i} + \eta_i, \eta_i \sim \mathcal{N}(0, \sigma^2) \implies L_0^{(0)}(y_i) = \frac{2y_i}{\sigma^2}$. Т.к. все $c_i = 0$.
$M[L_0^{(0)}(y_i)] = \mu_{00} = \frac{2}{\sigma^2}$. $D[L_0^{(0)}(y_i)] = \frac{4}{\sigma^2} = 2M[L_0^{(0)}(y_i)]$

Предположим, что все ЛОПП имеют нормальное распределние $\mathcal{L}_\lambda^{(i)} \sim N(\mu_{\lambda,i}, 2\mu_{\lambda,i}), 0 \le i < 2^\lambda, 0 \le \lambda \le m$

$$\mu_{\lambda,2i} = \Theta(\mu_{\lambda-1,i}) = \phi^{-1}\left(1 - (1 - \phi(\mu_{\lambda-1,i}))^2\right)$$
$$\mu_{\lambda,2i+1} = 2\mu_{\lambda-1,i}$$
$$\phi(x) = 1 - \frac{1}{\sqrt{4\pi x}} \int_{-\infty}^{\infty} \tanh \frac{u}{2} e^{-\frac{(u-x)^2}{4x}} du$$

Замораживаются символы с наименьшим $\mu_{m,i}$

Пример. Кусочно-квадратичная аппроксимация

$$\Theta(x) \approx \begin{cases} 0.9861x - 2.3152 & , x > 12 \\ x(9.005 \cdot 10^{-3} x + 0.7694) - 0.9507 & , x \in (3.5, 12] \\ x(0.062883x + 0.3678) - 0.1627 & , x \in (1, 3.5) \\ x(0.2202x + 0.066448) & , \text{иначе} \end{cases}$$

Доделать Картинка

10 Конструкция Плоткина и коды Рида-Маллера

Теорема 10.1. Пусть даны (n, k_i, d_i) коды $C_i, i = 0, 1$. $C = \{(c_1 + c_0, c_1) | c_i \in C_i\}$ – код $(2n, k_1 + k_0, \min(2d_1, d_0))$

Определение. Код Рида-Маллера $RM(r, m)$ длины 2^m порядка r – полярный код с $\mathcal{F} = \{i | 0 \leq i < 2^m, wt(i) < m - r\}$

Размерность $k = \sum_{i=m-r}^{m} C_m^i = \sum_{i=1}^{r} C_m^i$. Минимальное расстояние $d = 2^{m-r}$

Теорема 10.2. Минимальное расстояние d полярного кода длины $n = 2^m$ с замороженным множеством $\mathcal{F}$ равно $\min_{i \notin \mathcal{F}} 2^{wt(i)} = \min_{i \notin \mathcal{F}} wt(A_m^{(i)})$, где вес целого числа – число его ненулевых битов, $A_m^{(i)}$ – i-ая строка A_m

11 Минимальное расстояние кодов Рида-Маллера, БЧХ и полярных

Доделать Таблица

Замечание. Полярные коды не фонтан