Лекций 5

Ilya Yaroshevskiy

29 сентября

Содержание

1 Сверточные коды

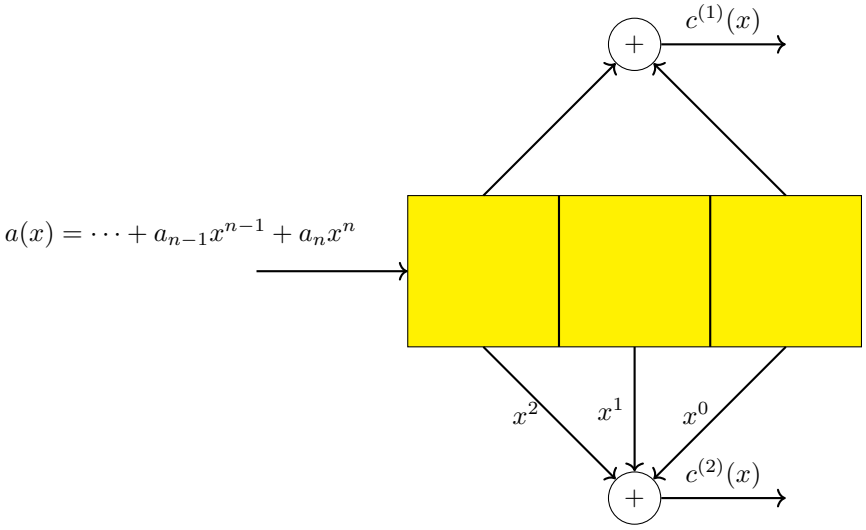
Замечание. Задача кодера – сделать передаваемые символы статистически зивисимыми

- Блоковые коды: функциональное преобразование блоков данных в кодовые слова
- Сверточные коды: автоматное отображение блоков данных в кадры колового слова

Простейший автомат – регистр сдвига. Кодер может хранить m ранее поступивших блоков из k_0 символов. На каждом шане кодер выдает n_0 закодированных символов. Скорость кода $R = \frac{k_0}{n_0}$. Объем памяти кодера – длина кодового ограничения $K = mk_0$.

Пример.

- $k_0 = 1, m = 2, K = k_0 m = 2, n_0 = 2$
- $g^{(1)}(x) = x^2 + 1, g^{(2)}(x) = x^2 + x + 1$



1.1 Порождающая матрица сверточного кода

Замечание. $k_0 = 1$: Выходная последовательность – линейная свертка информационной последовательности и порождащих многочленов кода

$$c^{(i)}(x) = c_0^{(i)} + c_1^{(i)}x + \cdots = a(x)g^{(i)}(x) = \sum_{j\geq 0} x^j \sum_{t=0}^{m} a_{j-t}g_t^{(i)}, 1 \leq i \leq n_0$$

Теоретически кодовые слова имеют бесконечную длину. В практических системах длина кодового слова фиксирована. В конец информационной последовательности вводят несколько дополнительных битов, переводящих регистр сдвига в нулевое состояние.

Кодирование в общем случае

$$(c^{(1)}(x), \ldots, c^{(n_0)}) = (a^{(1)}(x), \ldots, a^{(k_0)}(x))G(x)$$

$G(x)$ – $k_0 \times n_0$ порождающая матрица (многочленная) кода

Замечание. Сверточные коды являются линейными

Замечание. Графическое представление сверточных кодов:

- Последовательности возможных переходов конечного автомата могут быть представлены в виде дерева. Древовидная диаграмма обладает свойством самоподобия
- Решетчатая диаграмма – боле компактный способ задания кода
- Кодовое слово – путь в решетке, начинающийся и заканчивающийся в нулевом состоянии. Фиксированная длина. Предполагается, что после обработки информационной последовательности были поданы несколько дополнительных битов, переводящих регистр сдвига в нулевое состояние

1.2 Корректирующая способность

Определение. Минимальное расстояние Хемминга для любых последовательностей из l кадров, отличающихся начальным кадром, называется **l-м минимальным расстоянием кода** d_l^*.

Обозначение. d_{m+1}^* – минимальное расстояние кода

Определение. Последовательность $d_1^*, d_2^*, d_3^*, \ldots$ называется **дистанционным профилем кода**

Утверждение. *Если в первых l кадрах произошло t ошибок, то первый кадр может быть исправлен при условии $2t + 1 \leq d_l^*$*

Определение. Минимальное свободное расстояние кода $d_{\text{frcc}} = \max_l d_l^*$

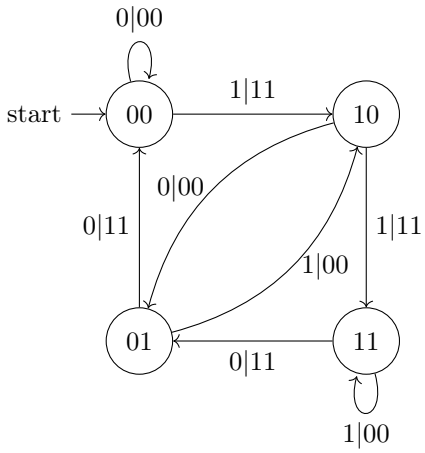
Замечание. Свободная длина n_{rfcc} кода – длина имеющего наименьший вес ненулевого начального сегмента кодовой последовательности сверточного кода

1.3 Катастрофические кодеры (порождающие матрицы)

Определение. Катастрофический кодер отображает информационные последовательности бесконечного веса в кодовые последовательности конечного веса

Замечание. КК характеризуется наличием петель нулевого веса в графе переходов

Пример. Порождающая матрица катастрофического кодера $G(x) = (x^2+1, x^2+1)$. Единичные ошибки в канале могут привести к бесконечному числу ошибок декодера. Если при передаче нулевого кодового слова возникла ошибка вида $\ldots 00011000 \ldots$, то она будет продекодирована в информационную последовательность вида $\ldots 000101010101 \ldots$, то она будет продекодирована в информационную последовательность вида $\ldots 000101010101 \ldots$



Замечание. Ошибка декодирования при исользовании некатастрофического кодера приводит к ограниченному числу ошибок на выходе декодера

Теорема 1.1. Порождающая матрица не является катастрофической ттогда, когда НОД определителей всех $k_0 \times k_0$ подматриц $G(x)$ равен $x^s, s \geq 0$.

1.4 Систематическое кодирование

Определение. Систематическое кодирование – информационная последовательность является подпоследовательностью кодовой последовательности

Любой сверточный код может быть преобразован к эквивалентному систематическому коду за счет введения фильтра с бесконечным импульсным откликом. Это преобразование информационной последовательности является биективным и не влияет на корректирующие свойства кода.

Утверждение. *Порождающая матрица $G(x)$ может быть приведена к каноническому виду аналогично случаю линейных блоковых кодов (Преобразование над полем рациональных функций)*

Некоторые информационные последовательности конечного веса могут попродить кодовые слова бесконечного веса

$$G(x) = (x^2 + 1, x^2 + x + 1) \to \left(\frac{x^2 + 1}{x^2 + x - 1}, 1 \right)$$

Доделать Картинка

Пример. $a(x) = 1 + x^4 + x^5; a(x)G(x) = [1 + x + x^2 + x^5, 1 + x^4 + x^5]$

шаг	вход	содержимое регистра	выход 0	выход 1
0	1	100	1	1
1	1	010	0	1
2	0	101	0	0
3	0	110	1	0
4	0	011	1	0
5	1	001	1	1

2 Декодирование сверточных кодов

2.1 Алгоритм Витерби

Декодирование по критерию максимума праводоподобия (= минимального расстояния). Кодовые слова соответсвуют путям в решетке

Пример. Доделать Картинка

2.2 Производящая функция

Замечание. Вероятность ошибки декодирования кода определяется числом кодовых слов различного веса. Число путей в решетке, начинающихся и заканчивающихся в нулевом состоянии

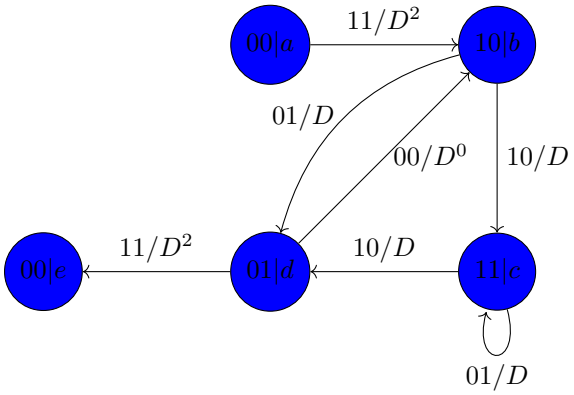
Пометим ребра графа переходов метками D^i, где i – вес кодовой последовательности. Последовательность символов веса x характеризуется одночленом D^x. Совокупность кодовых слов характеризуется многочленом, например $2D^6 + 3D^8$. Расщепим исходное состояние на два: начальное (0) и конечное (e). Пусть X_i характеризует совокупность кодовых последовательностей, приводящих кодер в состояние i. X_i – ряд, коэффициенты которого равны числу кодовых последовательностей, начинающихся в нулевом и заканчивающихся в i-ом состоянии. Производящая функция $T(D)$ равна X_e/X_a. Это степенной ряд, коэффициенты которого равны числу кодовых слов различного веса, выходящих из нулевого состояния и возвращающихся в него

Степень нунелувого члена – минимальное свободное расстояние кода. Минимальное свободное расстояние пропорционально длине кодового ограничения. При фиксированной длине блока сверточные коды хуже аналогичных блоковых

Пример.

$$\begin{cases} X_b = D^2 X_a + X_d \\ X_c = DX_b + DX_c \\ X_d = DX_c + DX_b \\ X_e = D^2 X_d \end{cases}$$

$$T(D) = \frac{D^5}{1-2D} = D^5 + 2D^6 + 4D^7 + 8D^8$$



2.3 Расширенная производящая функция

Исследуем зависимость веса кодового слова от веса информационной последовательности. Пометим ребра графа переходов метками $N^j D^i$, где i – вес выходной последовательности

- $j = 0$ – переход по 0
- $j = 1$ – переход по 1

Определение. Расширенная производящая функция – степенной ряд от переменных N и D, в котором коэффициент при $N^a D^b$ равен числу кодовых последовательностей веса b, порождаемых информационными последовательностями веса a.

Пример.

$$\begin{cases} X_b = ND^2 X_a + ND^0 X_d \\ X_c = NDX_b + NDX_c \\ X_d = DX_c + DX_b \\ X_e = D^2 X_d \end{cases}$$

$$T(D) = \frac{ND^5}{1-2D} = ND^5 + 2N^2D^6 + 4N^3D^7 + 8N^4D^8$$

Доделать Картинка ez

2.4 Вероятность ошибки декодирования (канал с АБГШ)

Вероятность ошибки декодирования (канал с АБГШ)

$$r_{ij} = (-i)^{c_{ij}} + \eta_{ij}, \eta_{ij} \sim N(0, \sigma^2), 1 \le j \le n_0, i = 0, 1, \dots$$

Предположим, что передавалосб нулевое кодовое слово. Будем считать, что алгоритм Витерби ищет последовательность с максимальной корреляцией $C = \sum_{i \ge 0} \sum_{j=1}^{n_0} r_{ij}(-1)^{c_{ij}}$.

Оценим вероятность первого события неправильного декодирвания. Ошибка произойдет, если при слиянии нескольких путей на некотором ярусе B окажется, что $C_1 > C_0$. $_0$ – метрика ненулевого пути c_{ij}, C_1 – метрика нулевого пути

$$P\{C_1 > C_0\} = P\left\{\sum_{i=0}^{B}\sum_{j=1}^{n_0} r_{ij}((-1)^{c_{ij}} - 1) > 0)\right\} = P\left\{\sum_{i=0}^{B}\sum_{j:c_{ij}\neq 0} r_{ij} < 0\right\}$$

Объединенная верхняя граница вероятности ошибки декодирования:

- $r_{ij} \sum N(1, \sigma^2)$

Если неправильный путь имеет вес d на ярусах $0, \dots, B$, то:

$$p = \sum_{i=0}^{B}\sum_{j:c_{ij}\neq 0} r_{ij} \sim N(d, d\sigma^2), \sigma^2 = \frac{N_0}{2}$$

$$P_d = P\{p < 0\} = Q\left(\sqrt{2d\frac{E_b}{N_0}}\right) = Q\left(\sqrt{2dR\frac{E_b}{N_0}}\right), Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-t^2/2}dt = \frac{1}{2}\mathrm{erfc}(x/\sqrt{2})$$

Вероятность ошибки – вероятность того, что будет выбран какой-либо неправильный путь

$$P_C = P\{(C_1 > C_0) \vee (C_2 > C_0) \vee \dots\} \le \sum_i P\{C_i > C_0\} = \sum_{d>0} t_d P_d = \sum_{d=d?}^{\infty} t_d Q\left(\sqrt{2dR\frac{E_b}{N_0}}\right)$$

Производящая функция $T(D) = \sum_{d \ge 0} t_d D^d$

Вероятность ошибки на бит в случае выборп ошибочного пути C_i с кодовой и информационной последовательности отичающихся от истснных в d и w позициях, соответсвенно, равна $\frac{w}{k_0}P\{C_i > C_0\} = \frac{w}{k_0}P_d$. Расширенная производящая функция $T(N, D) = \sum_{w,d} t_{wd} N^w D^d$.

$$t(D) = \left.\frac{\partial T(N,d)}{\partial N}\right|_{N=1} = \sum_d D^d \underbrace{\sum_w t_{wd} w}_{b_d}$$

Общая вероятность ошибки декодирования на бит

$$P_b \le \frac{1}{k_0}\sum_{d=d_{f?}}^{\infty} b_d Q\left(\sqrt{2dR\frac{E_b}{N_0}}\right)$$

2.5 Выводы

Сверточные коды – понятийно простой способ помехозащиты. Сложность декодирования алгритмом Витерби растет экспоненциально с длиной кодового ограничения и линейно с длиной кодируемой последовательности. Минимальное свободное расстояние растет с длиной кодового ограничения.

3 Комибинирование кодов

3.1 Конструкция Плоткина

Теорема 3.1. Пусть даны (n, k, d) коды $C_i, i = 1, 2$, $C = \{(c_1, c_1 + c_2) | c_i \in C_i, i = 1, 2\}$ – $(2n, k_1 + k_2, \min(2d_1, d_2))$ код

Доказательство. C содержит кодовые слова $(c_1, c_1), c_1 \in C_1, (0, c_2), c_2 \in C \implies d \le 2d_1, d \le d_2$

- Пусть $c_1, c_1' \in C_1 \setminus \{0\}, c_2, c_2' \in C_2 \setminus \{0\}$ – ненулевые кодовые слова компонентных кодов

$$d((c_1, c_1 + c_2), (c_1', c_1' + c_2')) = d(c_1, c_1') + d(c_1 + c_2, c_1' + c_2')$$

$$c_2 = c_2' \wedge c_1 \neq c_1' \implies d(c_1, c_1') + d(c_1 + c_2, c_1' + c_2') = d(c_1, c_1') + d(c_1, c_1') \leq 2d_1$$

$$\begin{aligned} c_2 \neq c_2' \implies d(c_1, c_1') + d(c_1 + c_2, c_1' + c_2') &= \mathrm{wt}(c_1 - c_1') + \mathrm{wt}(c_1 - c_1' + c_2 - c_2') \geq \\ &\geq \mathrm{wt}(c_1 - c_1') + \mathrm{wt}(c_2 - c_2') - \mathrm{wt}(c_1 - c_1') = \mathrm{wt}(c_2 - c_2') \geq \\ &\geq d_2 \end{aligned}$$

□

3.2 Декодирование кодов

Декодирование $(y', y'') = (c_1, c_1 + c_2) + (e', e'')$ в метрике Хемминга

$$y''' = y'' - y' = c_1 + c_2 + e'' - c_1 - e' = c_2 + e'''$$

Продекодируем y''' декодером кода C_2. Если $\mathrm{wt}((e', e'')) \leq \lfloor (d-1)/2 \rfloor$, то $\mathrm{wt}(e''') \leq \mathrm{wt}(e') + \mathrm{wt}(e'') \leq \lfloor (d-1)/2 \rfloor \leq \lfloor (d_2 - 1)/2 \rfloor$ и декодирование выполняется правильно&

Пусть c_2 найдено правильно. Продекодируем в C_1 вектора $y' = c_1 + e'$ и $y'' - c_2 = c_1 + e''$. Если $\mathrm{wt}((e', e'')) = \mathrm{wt}(e') + \mathrm{wt}(e'') \leq \lfloor (d-1)/2 \rfloor \leq \lfloor (2d_1 - 1)/2 \rfloor < d_1$, то $\mathrm{wt}(e') \leq \lfloor (d_1 - 1)/2 \rfloor \vee \mathrm{wt}(e'') \leq \lfloor (d_1 - 1)/2 \rfloor \implies$ декодирование y' или y'' даст правильный результат

3.3 Коды Рида-Маллера

Замечание. Рекурсивное применение конструкции Плоткина

- $RM(r, m)$ – код Рида-Маллера порядка r длины 2^m
- $RM(0, m) = (2^m, 1, 2^m)$
- $RM(m, m) = (2^m, 2^m, 1)$
- $RM(r+1, m+1)$ применение конструкции Плоткина к $C_1 = RM(r+1, m), C_2 = RM(r, m)$