Теория кодирования (определения и заметки)

Владимир Латыпов
donrumata03@gmail.com

Vladimir Latypov
donrumata03@gmail.com

Содержание

1 Базовые определения

Кодер источника — убирает избыточность (например, архиватор или jpeg), может быть с потерями.

Кодер канала — вносит контроллируемую избыточность.

Канал — вероятностная модель передачи данных, определяется $P(Y \mid X)$, где X — данные, непосредственно передающиеся, Y — принимаемые данные на выходе канала.

1.1 Декодирование

- По критерию идеального наблюдателя: минимизация P_e за счёт выбора в каждой точке x, наиболее вероятного при условии y (т.е. $\max_x p(x \mid y)$).
- По максимуму правдоподобия — выбор для x области, где его правдоподобие $p(y \mid x)$ выше других x: $\max_x p(y \mid x)$.

При $P(x) = \text{const}$ критерии эквивалентны.

1.2 Отношение сигнал-шум

$E_s = \alpha^2$

$P_{\text{noise}} \sim \sigma^2 = \frac{N_0}{2}$ (N_0 — спектральная плотность мощности шума, берём половину, т.к. комплексная часть не интересует)

На символ: $\frac{E_s}{N_0}$

На бит: $\frac{E_b}{N_0} = \frac{E_s}{N_0 R}$

Принято измерять в децибелах: $10 \log_{10}\left(\frac{E_b}{N_0}\right)$

Для 2-AM: $P_e = Q\left(\sqrt{2\frac{E_b}{N_0}}\right)$

1.3 Код

Определение 1.3.1 *(Код)* Множество $\mathcal{C}$ допустимых кодовых последвоательностей алфавита X (на практике — они блоковые)

Определение 1.3.2 *(Кодер)* Отображение $\mathcal{B}^n \hookrightarrow \mathcal{C}$

Определение 1.3.3 *(Скорость кода)* Отношение длины кодовой и исходной последовательностей

1.4 Дублирование

Если m раз продублировать каждый символ, то $P_e = Q\left(\sqrt{2m\frac{E_b}{N_0}}\right)$, но $R = \frac{1}{m}$, т.ч. если смотреть в пересчёте на бит — прироста нет.

1.5 Теоремы Шеннона

Есть трейдофф между скоростью и ошибками.

Теорема 1.5.4 *(Прямая теорема Шеннона)* Оказывается, что со скоростью, сколь угодно близкой к C, но меньшей C можно достигать сколь угодно малые P_e начиная с некоторой длина блока кода.

Теорема 1.5.5 *(Обратная теорема Шеннона)* Если $R > C$, то P_e ограничена снизу.

т.е. теоретический результат идеален. Теорема не конструктивна, но знаем, как достичь. Но:

- декодеры неэффективны
- конкретные (не асимптотические) вероятности ошибок плохие

btw случайные коды реализуют теорему Шеннона ;)

Пропускная способность канала —

$$C = \max_{P(x)} I(X;Y)$$

, где $I(X;Y) = H(Y) - H(Y \mid X)$ — *определяется через свойства канала*.

Источники субоптимальности:

- конечность длины блока
- несовершенство кода
- субоптимальность декодера
- дискретизация выхода канала

1.6 Жёсткое vs мягкое декодирование

Жёсткое — декодер использует жёсткие оценки для каждого символа.

- Тогда АБГШ $\longrightarrow$ BSC

Мягкое — декодер использует вероятности для каждого символа/напрямую принятое значение.

1.7 Спектральная эффективность

$\beta = \frac{R}{W}$ — число бит на Гц ширины спектра.

1.8 Декодирования

Списочное декодирование — декодер возвращает не один, а несколько вариантов.

Побитовое — часто используются L_i — лог. отношения правдоподобия — логарифм отношения вероятности всех слов с 1-цей ко всем словам с нулём на этой позиции. *То есть зависит и от остальных прянятых символов*. Используется

1.9 Критерий минимального расстояня: выбор ближайшего кодового слова к принятому.

2 Блоковые коды

Если минимальное расстояние — d:

- Внутри шара радиуса $d-1$ нет других кодовых слов $\longrightarrow$ Находит $d-1$ ошибок
- Шары радиуса $\lfloor\frac{d-1}{2}\rfloor$ не пересекаются $\longrightarrow$ Исправляет $\lfloor\frac{d-1}{2}\rfloor$ ошибок

3 Линейные коды

q-ичный код (n,k,d) — k-мероное подпространство $\mathrm{GF}(q)^n$ с минимальным расстоянием d.

Можно задать порождающей матрицей $G \in \mathrm{GF}^{k\times n}$, код — «образ» — все линейные комбинации строк G.

Можно задать проверочной матрицей $H \in \mathrm{GF}(q)^{r\times n}$, т.ч. $r \geq n-k = \operatorname{rank} H$, код — её «ядро» $Hx^T = 0 \iff xH^T = 0$.

Столбцы H — это базис ортогонального дополнения к коду, т.е. $GH^T = 0$.

Домножение слева на обратимую матрицу не меняет кода.

Домножение G справа на перестановочную переставляет сигнальные символы $\overset{\text{def}}{\iff}$ коды эквивалентны.

3.1 Систематическое кодирование

$G = (I_k \mid A)$, где I_k — единичная матрица. Проверочная матрица к ней: $H = (A^T \mid -I_{n-k})$.

Любой код можно привести к систематическому виду с точностью до эквивалетного: операциями над строками + перестановой столбцов.

3.2 Размерность и расстояние кода по проверочной матрице

3.3 Граница Синглтона

$n-k \geq d-1$

3.4 Код Хэминга

3.5 Синдромное декодирование

У каждого класса смежности $\mathrm{GF}(q)^n$ по аддитивной подгруппе кода — находим вектор ошибок минимального веса.

Классы определяются синдромом — $s = yH^T = (x+e)H^T = u\underbrace{GH^T}_{0} + eH^T = eH^T$.

3.6 Любопытные факты

Коды БЧХ < коды Гоппы < альтернантные код

Ещё один факт: расширение кода увеличивает максимальное расстояние на 1, если оно было нечётным, т.к. тогда все слова веса d увеличат вес на 1.

- После итерации i декодирования обобщённых каскадных кодов столбцы закодированы в коде B_{i+1}, т.к. мы вычитаем вклад B_i из каждого столбца j: $c_j B_i^T$, где B_i — матрица добавки i-того кода.
- В минимальной решётке создаём узлы только для различных таких множеств (для классов эквивалетности прошлых по совпадению будущих). Узлы соединяем, если существует кодовое слово т.ч. прошлое для одного и другого узла — его префиксы. Тогда ребро помечаем i-м элементом этого кодового слова.
- Как расписывать БКЕР:
  - Постановка задачи
  - Выражение L_i
  - Расписывание вероятности $p(s_i = s', s_{i+1} = s, y_0^{n-1})$ через α, β, γ
  - α и β обычные и штрихованные: определения, рекурсивные формулы. В выражении α' используется α_{i-1}, но не страшно, т.к. общие их делители сокращаются.
  - Вычисление γ
  - Финальный алгоритм
- В Тала-Варди для каджого начала кодового слова поддерживаются массивы представлений в виде кодов Плоткина и ЛОППов, в сумме размера порядка n.