ЛАБОРАТОРНАЯ РАБОТА №5

Декодирование сверточных кодов, минимизирующее вероятность ошибки на символ

Алгоритм Витерби декодирования сверточного кода, рассмотренный в лабораторной работе 4, представляет собой алгоритм декодирования по максимуму правдоподобия, минимизирующий вероятность ошибочного слова на выходе декодера. Однако этот алгоритм необязательно минимизирует вероятность ошибки на символ (бит) слова сверточного кода.

В настоящей лабораторной работе будет рассмотрен оптимальный алгоритм декодирования сверточного кода, минимизирующий вероятность ошибки на символ (бит) слова сверточного кода. Этот алгоритм был предложен в 1974 году Л. Р. Балом, Дж. Куком, Ф. Джелинеком и Дж. Равивом. Практическое значение этого алгоритма состоит не только в том, что он обеспечивает меньшую вероятность ошибки на бит (по этому параметру выигрыш по сравнению с алгоритмом Витерби получается небольшим). Важно, что в результате декодирования формируются оценки надежности каждого декодированного информационного или кодового символа. Эти оценки затем используются в каскадных схемах для мягкого декодирования внешних кодов. Кроме того, на основе таких оценок строятся схемы многократного (итеративного) декодирования, относительно недавно получившие название «турбо-декодирование».

5.1. Описание метода декодирования

Проиллюстрируем постановку задачи декодирования по максимуму апостериорной вероятности (МАВ) с помощью следующего примера.

Пример 5.1. Рассмотрим сверточный код со скоростью $R = 1/n = 1/2$ и кодовым ограничением $\nu = 2$, задаваемый генераторными полиномами $\mathbf{g}_1 = (111)$ и $\mathbf{g}_2 = (101)$. Решетчатая диаграмма кода приведена на рис. 1.4. (лаб. раб. 1). Для произвольной последовательности $\mathbf{a} = (a_1,...,a_n)$ через $\mathbf{a}_i^j$, $1 \le i \le j \le n$, мы обозначаем подпоследовательность $\mathbf{a}_i^j = (a_i,...,a_j)$. Предположим, что информационная последовательность $\mathbf{i}_1^\tau$=(010100) длины $\tau = 6$ состоит из $T = 4$ информационных символов, за которыми следует $\nu = 2$ нулей. Она кодируется указанным выше сверточным кодом. Соответствующее кодовое слово длины $l = n\tau = 12$ имеет вид $\mathbf{x}_1^\tau = (\mathbf{x}_1,...,\mathbf{x}_\tau) =$ (00 11 10 00 10 11). В решетчатой диаграмме кода ему соответствует путь, содержащий 6 ребер, начинающийся и заканчивающийся в нулевом состоянии $(S_0 = 0, S_\tau = 0)$. Кодовое слово передается по дискретному каналу без памяти, $\mathbf{y}_1^\tau$ обозначает выходную последовательность канала, соответствующую входной последовательности $\mathbf{x}_1^\tau$. При декодировании по максимуму правдоподобия (МП), например, с помощью алгоритма Витерби, будет выбрано некоторое кодовое слово и соответствующие ему информационные символы будут результатом работы декодера. Более сложная задача – для каждого $t = 1,...,6$ вычислить вероятности информационных символов $i_t = 0$ или $i_t = 1$ при заданной последовательности $\mathbf{y}_1^\tau$. То из двух значений, которое имеет большую апостериорную вероятность является решением МАВ-декодера. Понятно, что его решение, вообще говоря, не совпадает с решением, принимаемым МП-декодером.

Предположим, что дискретный канал без памяти задается переходными вероятностями $p(y_t^{(j)} \mid x_t^{(j)})$, где $x_t^{(j)}, y_t^{(j)}$ – соответственно j-й входной и j-й выходной символы блока с номером t (этот блок соответствует некоторому ребру решетчатой диаграммы, соединяющему узлы ярусов с номерами $t-1$ и t). Тогда переходные вероятности для блоков символов (ребер решетчатой диаграммы) определяются по формуле

$$p(\mathbf{y}_t \mid \mathbf{x}_t) = \prod_{j=1}^{n} p(y_t^{(j)} | x_t^{(j)}) .$$

В случае двоичного симметричного канала (ДСК) с переходной вероятностью p, вероятности $p(\mathbf{y}_t \mid \mathbf{x}_t)$ вычисляются по формуле $p(\mathbf{y}_t \mid \mathbf{x}_t) = p^d (1-p)^{n-d}$, где d – расстояние Хэмминга между $\mathbf{x}_t$ и $\mathbf{y}_t$.

Пусть $\mathbf{y}_1^\tau$ обозначает выходную последовательность канала, соответствующую входной последовательности $\mathbf{x}_1^\tau$. Тогда для всех t, $1 \le t \le \tau$ имеем

$$p(\mathbf{y}_1^t \mid \mathbf{x}_1^t) = \prod_{j=1}^{t} p(\mathbf{y}_j \mid \mathbf{x}_j) .$$

Цель MAB-декодера или декодера БДКР (Бала-Джелинека-Кука-Равива) – при известной последовательности на выходе канала $\mathbf{y}_1^\tau$ при каждом $t = 1,...,\tau$ максимизировать следующую апостериорную вероятность

$$\Pr\{i_t \mid \mathbf{y}_1^\tau\} = \frac{\Pr\{i_t, \mathbf{y}_1^\tau\}}{\Pr\{\mathbf{y}_1^\tau\}} ,$$

где i_t – информационный символ, поступающий на вход кодера в момент времени t.

Так как принятая последовательность $\mathbf{y}_1^\tau$ фиксирована, то достаточно максимизировать совместную вероятность $\Pr\{i_t, \mathbf{y}_1^\tau\}$ или, другими словами, найти

$$\hat{i}_t = \arg\max_{i_t} \Pr\{i_t, \mathbf{y}_1^\tau\}.$$

Информационный символ i_t, $1 \le t \le \tau$ при известном состоянии кодера $S_{t-1} = m'$ в момент $t-1$ однозначно определяет состояние S_t кодера в момент t или, иначе можно сказать, что для каждой последовательности состояний существует единственный путь в решетчатой диаграмме. Вместо оптимальной информационной последовательности удобнее искать соответствующую ему оптимальную последовательность состояний. Таким образом, декодеру, минимизирующему вероятность ошибки на символ, вместо подсчета вероятности $\Pr\{i_t, \mathbf{y}_1^\tau\}$ достаточно вычислить вероятность $\Pr\{S_t = m \mid \mathbf{y}_1^\tau\}$, соответствующую каждому узлу в решетке сверточного кода и вероятность перехода из состояния S_{t-1} в состояние S_t, $\Pr\{S_{t-1} = m', S_t = m \mid \mathbf{y}_1^\tau\}$, соответствующую каждому ребру сверточного кода.

Учитывая, что для заданного $\mathbf{y}_1^\tau$ вероятность $\Pr\{\mathbf{y}_1^\tau\}$ равна константе, достаточно, чтобы декодер вместо условных вероятностей вычислял следующие совместные вероятности

$$\lambda_t(m) = \Pr\{S_t = m, \mathbf{y}_1^\tau\}$$

и

$$\sigma_t(m', m) = \Pr\{S_{t-1} = m', S_t = m, \mathbf{y}_1^\tau\}.$$

Рассмотрим алгоритм получения вероятностей $\lambda_t(m)$ и $\sigma_t(m', m)$. Определим вспомогательные вероятности

$$\alpha_t(m) = \Pr\{S_t = m, \mathbf{y}_1^t\} ,$$

$$\beta_t(m) = \Pr\{\mathbf{y}_{t+1}^\tau \mid S_t = m\},$$

$$\gamma_t(m', m) = \Pr\{S_t = m, \mathbf{y}_t \mid S_{t-1} = m'\}.$$

Заметим, что эти вероятности зависят уже не от всей последовательности $\mathbf{y}_1^\tau$. Вероятность

$\alpha_t(m)$ зависит только от «прошлого», а $\beta_t(m)$ - только от «будущего». Это обстоятельство позволит получить для них удобные рекуррентные формулы. Вероятность $\gamma_t(m',m)$ вычисляется просто, поскольку зависит только от одного текущего ребра. Теперь нужно установить связь $\lambda_t(m)$ и $\sigma_t(m',m)$ с вспомогательными вероятностями α, β, γ. Нетрудно видеть, что искомые вероятности $\lambda_t(m)$ и $\sigma_t(m',m)$ могут быть представлены в виде

$$\begin{aligned}\lambda_t(m) &= \Pr\{S_t = m, \mathbf{y}_1^\tau\} = \\ &= \Pr\{S_t = m, \mathbf{y}_1^t\}\Pr\{\mathbf{y}_{t+1}^\tau \mid S_t = m, \mathbf{y}_1^t\} = \\ &= \alpha_t(m)\Pr\{\mathbf{y}_{t+1}^\tau \mid S_t = m\} = \\ &= \alpha_t(m)\beta_t(m)\end{aligned} \tag{5.1}$$

и

$$\sigma_t(m',m) = \alpha_{t-1}(m')\gamma_t(m',m)\beta_t(m). \tag{5.2}$$

Можно показать, что вспомогательные вероятности $\alpha_t(m)$ и $\beta_t(m)$ могут быть вычислены по следующим рекуррентным формулам

$$\alpha_t(m) = \sum_{m'=0}^{M-1}\alpha_{t-1}(m')\gamma_t(m',m) \tag{5.3}$$

$$\beta_t(m) = \sum_{m'=0}^{M-1}\beta_{t+1}(m')\gamma_{t+1}(m,m') \tag{5.4}$$

с начальными условиями

$$\begin{aligned}&\alpha_0(0) = 1,\ \alpha_0(m) = 0,\ m \neq 0, \\ &\beta_\tau(0) = 1,\ \beta_\tau(m) = 0,\ m \neq 0\end{aligned} \tag{5.5}$$

В формулах (5.3) и (5.4) M – это число узлов на каждом ярусе решетки сверточного кода. Теперь рассмотрим вероятность $\gamma_t(m',m)$:

$$\begin{aligned}\gamma_t(m',m) &= \Pr\{S_t = m, \mathbf{y}_t \mid S_{t-1} = m'\} = \\ &= \sum_{\mathbf{x}}\Pr\{S_t = m \mid S_{t-1} = m'\}\Pr\{\mathbf{x}_t = \mathbf{x} \mid S_{t-1} = m', S_t = m\}p(\mathbf{y}_t \mid \mathbf{x}) = \\ &= \sum_{\mathbf{x}} p_t(m \mid m')q_t(\mathbf{x} \mid m',m)p(\mathbf{y}_t \mid \mathbf{x}),\end{aligned} \tag{5.6}$$

где переходные вероятности решетчатой диаграммы $p_t(m \mid m') = 1/2$, $t \le T$ так как мы предполагаем, что все входные последовательности сверточного кода равновероятны для всех $t \le T$. Для $t > T$ возможен только один переход из каждого состояния и его вероятность $p_{t>T}(m \mid m') = 1$, выходной блок кодера $\mathbf{x}_t$ представляет собой детерминированную функцию перехода в решетчатой диаграмме, т.е. $q_t(\mathbf{x} \mid m,m')$ принимает значение 1, если при переходе из состояния m' в состояние m на выходе кодера формируется блок $\mathbf{x}$ и значение 0 в противном случае. Для постоянных во времени сверточных кодов функция $q_t(\cdot \mid \cdot)$ не зависит от t.

Как было сказано выше, в случае передачи по ДСК с переходной вероятностью p вероятность $p(\mathbf{y}_t \mid \mathbf{x}_t) = p^d(1-p)^{n-d}$, где d – расстояние Хэмминга между входным блоком $\mathbf{x}_t$ и выходным блоком $\mathbf{y}_t$.

Таким образом, мы можем сформулировать алгоритм для вычисления $\lambda_t(m)$ и $\sigma_t(m',m)$ декодером БДКР.

Алгоритм БДКР:

1. Инициализировать $\alpha_0(m)$ и $\beta_0(m)$, $m = 0,1,...,M-1$ в соответствии с (5.5).
2. («Прямой проход»). При получении очередного блока $\mathbf{y}_t$ вычислить $\gamma_t(m,m')$ по формуле (5.6) и $\alpha_t(m)$ по рекуррентной формуле (5.3). Вычисленные значения $\alpha_t(m)$ запомнить для всех t и m.
3. («Обратный проход»). После получения всей последовательности $\mathbf{y}_1^\tau$ вычислить $\beta_t(m)$, $t = 1,2,...,\tau$ по рекуррентной формуле (5.4).
4. Вычислить $\lambda_t(m)$ и $\sigma_t(m,m')$ по формулам (5.1) и (5.2).

Для завершения описания БДКР-декодера осталось сформулировать правило получения оценок информационных символов по известным $\lambda_t(m)$ и $\sigma_t(m',m)$.

Предположим, что $\lambda_t(m)$ вычислены. Обозначим через A_t множество состояний решетки S_t, соответствующих информационному символу $i_t = 0$. Тогда

$$\Pr\{i_t = 0, \mathbf{y}_1^\tau\} = \sum_{S_t \in A_t} \lambda_t(m).$$

Разделим обе части на $\Pr\{\mathbf{y}_1^\tau\} = \lambda_\tau(0)$ и получим

$$\Pr\{i_t = 0 \,|\, \mathbf{y}_1^\tau\} = \frac{1}{\lambda_\tau(0)} \sum_{S_t \in A_t} \lambda_t(m). \tag{5.5}$$

Декодер БДКР принимает решение, $i_t = 0$ если $\Pr\{i_t = 0 \,|\, \mathbf{y}_1^\tau\} \ge 0{,}5$ и решение $i_t = 1$ в противном случае.

В ряде случаев необходимо знать апостериорные вероятности не информационных, а кодовых символов, т.е. вероятности $\Pr\{x_t^{(j)} = 0 \,|\, \mathbf{y}_1^\tau\}$. Пусть $B_t^{(j)}$ обозначает множество переходов $S_{t-1} = m' \to S_t = m$ таких, что j-й выходной символ $x_t^{(j)}$=0. Очевидно, что для постоянных во времени сверточных кодов $B_t^{(j)}$ не зависит от t. Тогда

$$\Pr\{x_t^{(j)} = 0, \mathbf{y}_1^\tau\} = \sum_{(m',m) \in B_t^{(j)}} \sigma_t(m',m).$$

Эта вероятность может быть нормализована делением на $\lambda_\tau(0)$ для получения

$$\Pr\{x_t^{(j)} = 0 \,|\, \mathbf{y}_1^\tau\} = \frac{1}{\lambda_\tau(0)} \sum_{(m',m) \in B_t^{(j)}} \sigma_t(m',m).$$

По этой вероятности в свою очередь принимается решение о наиболее вероятном значении каждого кодового символа.

Пример 5.1 (продолжение). Вернемся к рассмотрению примера кода (7,5). Предположим, что переходная вероятность ДСК $p = 0.1$ и что при передаче кодовой последовательности $\mathbf{x}_1^\tau$= 00 11 10 00 10 11 мы получили из канала последовательность $\mathbf{y}_1^\tau$= 01 11 11 00 10 11. В таблице 5.1 приведены значения $\gamma_t(m',m)$, вычисленные по формуле (5.6). В таблице 5.2 приведены соответствующие значения $\alpha_t(m)$, вычисленные по рекуррентной формуле (5.3). В таблице 5.3 приведены соответствующие значения $\beta_t(m)$, вычисленные по рекуррентной формуле (5.4). В таблице 5.4 приведены значения $\lambda_t(m)$, полученные с помощью (5.1). В таблице 5.5 приведены значения вероятностей $\Pr\{i_t = 0 \,|\, \mathbf{y}_1^\tau\}$, вычисленные по формуле (5.5). Из результатов вычислений следует, что решение декодера о передаваемой информационной последовательности имеет вид 010100. Помимо информационной последовательности, в результате работы декодера получена информация о надежности принятых решений.

Таблица 5.1.

Вероятности $\gamma_t(m',m)$ для примера 5.1

Вероят-ности	Номер яруса t					
	1	2	3	4	5	6
$\gamma_t(0,0)$	$1/2p(1-p)=0.045$	$1/2p^2=0.005$	0.005	0.405	0.09	0.01
$\gamma_t(0,2)$	$1/2p(1-p)=0.045$	$1/2(1-p)^2=0.405$	0.405	0.005		
$\gamma_t(1,0)$			0.405	0.005	0.09	0.81
$\gamma_t(1,2)$			0.005	0.405		
$\gamma_t(2,1)$		$1/2p(1-p)=0.045$	0.045	0.045	0.81	
$\gamma_t(2,3)$		$1/2p(1-p)=0.045$	0.045	0.045		
$\gamma_t(3,1)$			0.045	0.045	0.01	
$\gamma_t(3,3)$			0.045	0.045		

Таблица 5.2.

Вероятности $\alpha_t(m)$ для примера 5.1

Вероят-ности	Номер яруса t					
	1	2	3	4	5	6
$\alpha_t(0)$	0.045	2.25×10^{-4}	8.205×10^{-4}	3.375×10^{-4}	3.44375×10^{-5}	0.00025
$\alpha_t(1)$		0.002025	9.125×10^{-4}	4.556×10^{-5}	3.0625×10^{-4}	
$\alpha_t(2)$	0.045	0.018225	1.0125×10^{-4}	3.75×10^{-4}		
$\alpha_t(3)$		0.002025	9.125×10^{-4}	4.556×10^{-5}		

Таблица 5.3.

Вероятности $\beta_t(m)$ для примера 5.1

Вероя т-ности	Номер яруса t					
	5	4	3	2	1	0
$\beta_t(0)$	0.01	0.0009	0.00365	1.82275×10^{-4}	0.00485	0.00024375
$\beta_t(1)$	0.81	0.0009	0.26575	0.001475		
$\beta_t(2)$		0.6561	0.000405	0.011975	0.0006	
$\beta_t(3)$		0.0081	0.000405	0.011975		

Таблица 5.4.

Вероятности $\lambda_t(m)$ для примера 5.1

Вероятности	Номер яруса t						
	0	1	2	3	4	5	6
$\lambda_t(0)$	$2.4\cdot10^{-4}$	$2.2\cdot10^{-4}$	$4.1\cdot10^{-8}$	$2.99\cdot10^{-6}$	$3.0\cdot10^{-7}$	$3.44\cdot10^{-7}$	$2.5\cdot10^{-4}$
$\lambda_t(1)$			$3.0\cdot10^{-6}$	$2.42\cdot10^{-4}$	$4.1\cdot10^{-7}$	$2.48\cdot10^{-4}$	
$\lambda_t(2)$		$2.7\cdot10^{-5}$	$2.18\cdot10^{-4}$	$4.1\cdot10^{-8}$	$2.46\cdot10^{-4}$		
$\lambda_t(3)$			$2.42\cdot10^{-5}$	$3.69\cdot10^{-7}$	$3.69\cdot10^{-7}$		

Таблица 5.5.

Апостериорные вероятности информационных символов для примера 5.1

Вероятность	Номер яруса t					
	1	2	3	4	5	6
$\Pr\{i_t = 0 \mid \mathbf{y}_1^\tau\}$	0.872	0.0126	0.980	0.0028	1	1

5.2. Порядок выполнения работы

1. В соответствии с вариантом задания выбрать сверточный кодер, модель канала, последовательность на выходе канала.
2. Построить решетчатую диаграмму кода и выполнить БДКР-декодирование. Результаты представить в виде таблиц аналогичных таблицам 5.1 – 5.3.

5.3. Контрольные вопросы

1. Укажите области применения декодера БДКР и декодера Витерби.
2. Оцените вычислительную сложность алгоритма БДКР и сравните со сложностью МП-декодирования.
3. Оцените объем памяти БДКР-декодера и сравните с объемом памяти декодера Витерби.
4. Декодирование по МП в ДСК сводится к декодированию по минимуму расстояния Хэмминга. Можно ли МАВ-декодирование упростить подобным образом?
5. Декодирование по МП в гауссовском канале сводится к декодированию по минимуму расстояния Евклида. Можно ли МАВ-декодирование в гауссовском канале упростить подобным образом?
6. Предположим, что БДКР-декодер используется как в каскадной схеме и после первой ступени декодирования уже известны некоторые априорные вероятности информационных символов. Что нужно изменить в приведенном выше описании алгоритма, чтобы учесть эту дополнительную информацию.