СИНДРОМНОЕ ДЕКОДИРОВАНИЕ. МЕТОД МАЖОРИТАРНОГО ДЕКОДИРОВАНИЯ.

Презентация к лекции по дисциплине
«Защита информации в системах радиосвязи и радиодоступа»

*Презентация доступна на Образовательном Портале ПГТУ в соответствующем курсе.

Изначально синдромное декодирование предназначено для обнаружения ошибок, т.е. для установления факта наличия ошибок в принимаемых кодовых комбинациях или в кодовых блоках.

Однако, в каналах с высоким отношением SNR т.е. с точной вероятностью обнаружения ошибок (Bit Error Rate), синдромное декодирование может быть расширено и для задач автоматического исправления ошибок. Это возможно, если количество синдромов не ниже числа векторов ошибок с предельным весом, определяемым кратностью исправления ошибок:

$$(N, K), \quad t_{\text{и}} = T, \quad N_{\text{ош}} = C_N^T, \quad M = N - K, \quad 2^M - 1 \geq C_N^T$$

Синдром вычисляется в результате скалярного произведения в двоичном пространстве принятого блока и транспонированной проверочной матрицы:

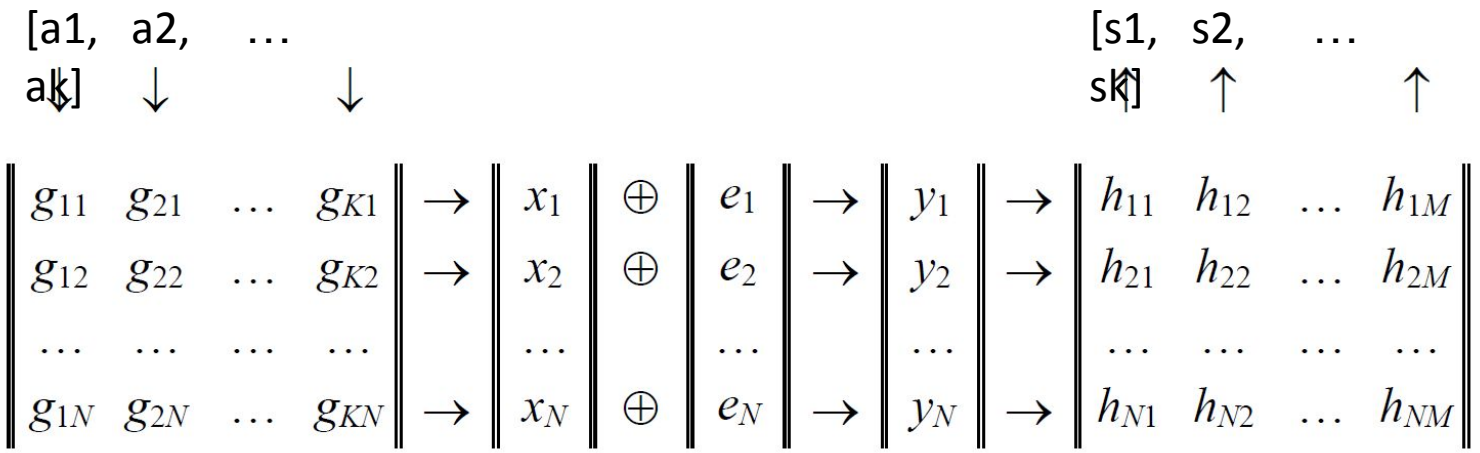
$$\underset{(N-K)\uparrow}{\vec{s}} = \underset{N\uparrow}{\vec{y}} \otimes \underset{\uparrow N\times(N-K)}{\vec{H}^T}$$

Произведение можно детализировать:

$$S_m = \left(\sum_{n=1}^{N} y_n \cdot h_{m,n} \right) mod2, \qquad m \in [1..(N-K)]$$

, где $\vec{y} = \vec{x} \oplus \vec{e}$, $\vec{x} = \vec{a} \otimes \vec{G}$, $\vec{x}_n = \sum_{k=1}^{K} a_k \cdot g_{k,n}$

Этот процесс достаточно просто и весьма информативно отображается схемой преобразований.



Для корректного декодирования необходимо, чтобы порождающая и проверочная матрицы однозначно соответствовали друг другу. Такое соответствие определяется условием:

$$\vec{G} \otimes \vec{H}^T = \vec{0}$$

В итоге структура синдрома зависит от структуры вектора ошибок:

$$\vec{s} = \vec{y} \otimes \vec{H}^T = (\vec{x} \oplus \vec{e}) \otimes \vec{H}^T = \left(\vec{x} \otimes \vec{H}^T\right) \oplus \left(\vec{e} \otimes \vec{H}^T\right) =$$
$$= \left(\vec{a} \otimes \vec{G} \otimes \vec{H}^T\right) \oplus \left(\vec{e} \otimes \vec{H}^T\right) = \left(\vec{a} \otimes \vec{0}\right) \oplus \left(\vec{e} \otimes \vec{H}^T\right)$$
$$= \vec{0} \oplus \left(\vec{e} \otimes \vec{H}^T\right) = \vec{e} \otimes \vec{H}^T$$

Таким образом, можно сделать вывод что синдром – это прямая реакция на вектор ошибок.

При этом надо иметь ввиду, что один и тот же синдром может соответствовать нескольким различным векторам ошибок, что не влияет на результат обнаружения, но затрудняет автоматическое исправление ошибок.

В общем случае между матрицами G и H действует конструктивное подобие. В двух частных случаях канонических форм порождающих матриц, конструктивное подобие имеет следующий вид.

1)

$$\underset{\uparrow K\times N}{\vec{G}} = \underset{\uparrow K\times K \uparrow K\times (N-K)}{[E \vdots P]} <=> \underset{\uparrow N\times (N-K)}{\vec{H}^T} = \begin{matrix} K\times(N-K)\downarrow \\ \begin{bmatrix} P \\ E \end{bmatrix} \end{matrix}_{\uparrow (N-K)\times(N-K)}$$

2)

$$\vec{G} = [P \vdots E] <=> \vec{H}^T = \begin{bmatrix} E \\ P \end{bmatrix}$$

Проверочная транспонированная матрица.

При использовании порождающей матрицы с явно выраженными подматрицами **E** и **P** проверочная матрица должна иметь соответствующую структуру с двумя аналогичными подматрицами, в данном случае

$$\mathbf{H^T} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1(N-K)} \\ p_{21} & p_{22} & \cdots & p_{2(N-K)} \\ \cdots & \cdots & \cdots & \cdots \\ p_{K1} & p_{K2} & \cdots & p_{K(N-K)} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = \begin{pmatrix} \mathbf{P} \\ \mathbf{E} \end{pmatrix}$$

При этом должно выполняться условие:

$$\mathbf{G} \bullet \mathbf{H}^{\mathrm{T}} = \mathbf{0}$$

означающее получение нулевого синдрома при отсутствии ошибок в канале передачи.

Если в векторе синдрома **s** имеется хотя бы одна 1, это является признаком обнаружения ошибки.

Формирование проверочной транспонированной матрицы.

Код (7,3), N=7, K=3

$$\vec{G} = \begin{matrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix}$$

На основании системы уравнений порождающих полиномов сформируем эквивалентную систему уравнений, состоящую из N-K = 4 выражений, определяющих проверку на чётность:

$$\begin{aligned} x_1 &= a_1 \\ x_2 &= a_2 \\ x_3 &= a_3 \\ x_4 &= a_1 \oplus a_2 \\ x_5 &= a_1 \oplus a_3 \\ x_6 &= a_2 \oplus a_3 \\ x_7 &= a_1 \oplus a_2 \oplus a_3 \end{aligned}$$

$$\begin{cases} x_1 \oplus x_2 \oplus x_4 = 0 \\ x_1 \oplus x_3 \oplus x_5 = 0 \\ x_2 \oplus x_3 \oplus x_6 = 0 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_7 = 0 \end{cases}$$

$$\vec{H} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \vec{H}^T = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Пример:

$$\vec{G} = \begin{matrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix}$$

$$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$$

$$x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6 \quad x_7$$

Синдромный декодер, как видно из базовой функции и структуры проверочной матрицы, можно реализовать и программно, и аппаратно.

$$\vec{H}^T = \begin{matrix} 1 & 1 & 0 & 1 \leftarrow y_1 \\ 1 & 0 & 1 & 1 \leftarrow y_2 \\ 0 & 1 & 1 & 1 \leftarrow y_3 \\ 1 & 0 & 0 & 0 \leftarrow y_4 \\ 0 & 1 & 0 & 0 \leftarrow y_5 \\ 0 & 0 & 1 & 0 \leftarrow y_6 \\ 0 & 0 & 0 & 1 \leftarrow y_7 \end{matrix}$$

$$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$$

$$s_1 \; s_2 \; s_3 \; s_4$$

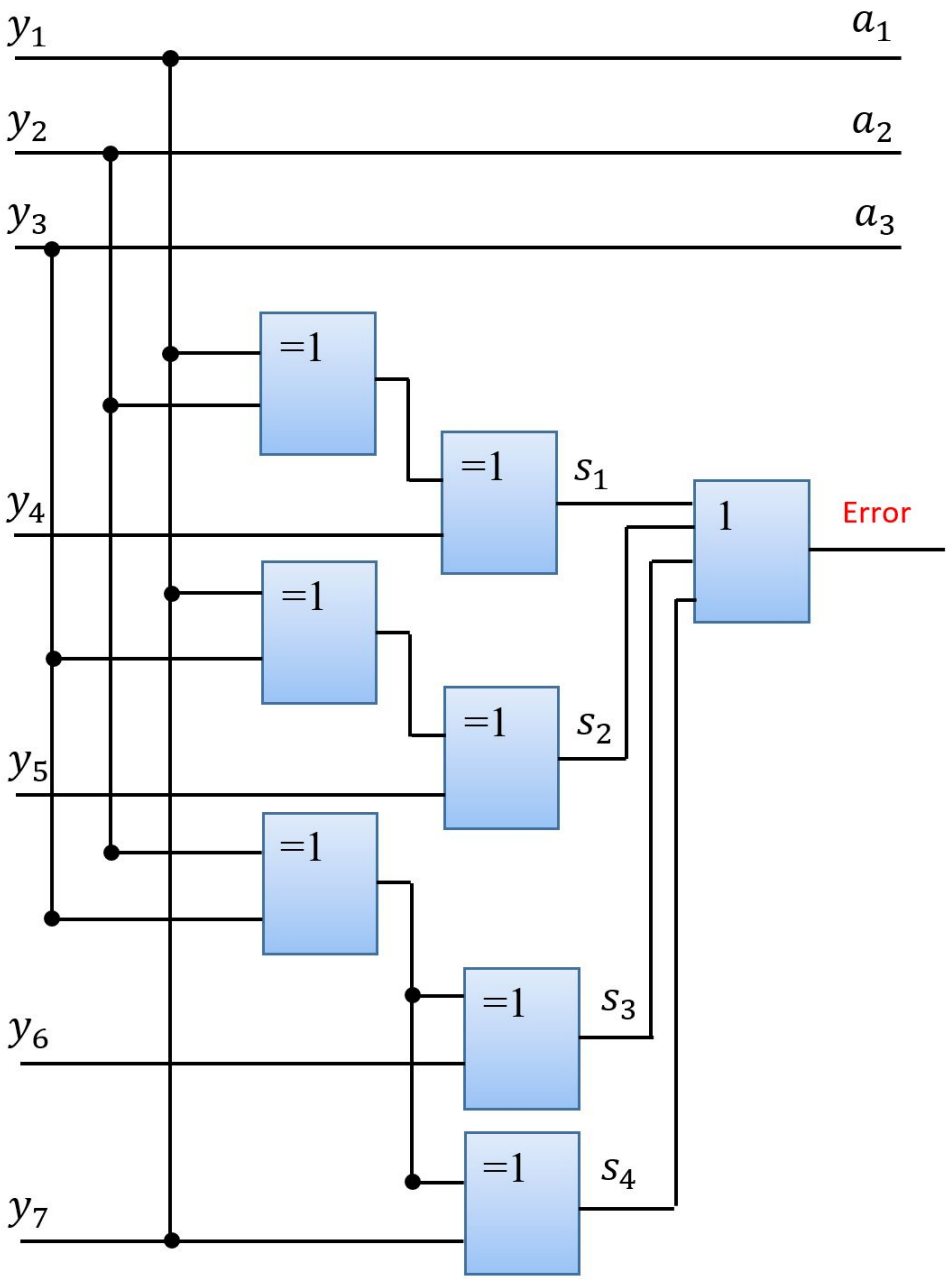
$$s_1 = y_1 + y_2 + y_4$$

$$s_2 = y_1 + y_3 + y_5$$

$$s_3 = y_2 + y_3 + y_6$$

$$s_4 = y_1 + y_2 + y_3 + y_7$$

Аппаратная реализация синдромного декодера:



Как видно из приведённой схемы, в сравнении со схемой соответствующего блокового кода, и кодер, и декодер имеют одинаковую основу.

Декодер отличается наличием дополнительных элементов проверок и выходного решающего элемента, с помощью которого формируется общий сигнал ошибок.

Мажоритарное декодирование систематических линейных блоковых кодов

Среди всех методов автоматического исправления ошибок наибольший интерес представляет метод мажоритарного декодирования. Метод реализуется на основе принятия окончательного решения по большинству частных оценок. Совокупности частных оценок и окончательные решения применяются только для информационных символов.

1) В силу этого, данный метод применятся только к систематическим кодам.
2) Кроме того, кратность исправления ошибок должна быть не нулевой: $t_{и} \geq 1$

Кроме того, целесообразно чтобы количество частных оценок для каждого из информационных элементов было одинаково.

Всей совокупности перечисленных условий соответствует только ограниченное количество классов кодов. Из них наиболее оптимальными являются коды на основе М-последовательности (Предельными способностями к обнаружению и исправлению ошибок при одной и той же длине кодовых слов обладают последовательности максимальной длины, или М-последовательности.).

М-последовательность – это код с параметрами:

$$(N, K, d_{min}) \equiv (2^K - 1, K, 2^{K-1})$$

Мажоритарное декодирование линейных блоковых кодов (ЛБК) основано на получении конечного набора оценок значений каждого из информационных символов на основе всех элементов кодовой комбинации и выборе той оценки, которая встречается в полученном наборе наиболее часто.

Например, в двоичном систематическом ЛБК (7, 3) - $N = 7$, $K = 3$, $d_{min} = 4$, $t_и = 1$, определяемом порождающей матрицей:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

процедуры формирования частных кодовых символов x_n, n=1..7, на основе информационных символов a_k, k=1..3, образуют систему выражений:

$$x_1 = a_1$$
$$x_2 = a_2$$
$$x_3 = a_3$$
$$x_4 = a_1 \oplus a_2$$
$$x_5 = a_1 \oplus a_3$$
$$x_6 = a_2 \oplus a_3$$
$$x_7 = a_1 \oplus a_2 \oplus a_3$$

Легко показать, что наборы оценок для каждого из трех информационных символов описываются системами выражений:

Оценки:			
1			
2			
3			
4			

Видно, что каждый из принятых символов y_i входит в частные оценки один раз, и, следовательно, если он ошибочен, то ошибочным будет одна из оценок. Решение об оценке состояния разряда принимается на основании большинства частных оценок.

Как видно из приведенных систем оценок, при оптимальном построении кода (точнее, его порождающей матрицы) количество частных оценок совпадает с весами Хэмминга строк порождающей матрицы, и каждый из кодовых символов одинаковое число раз участвует в формировании частных оценок. Данные свойства характерны для всех двоичных ЛБК класса (2^K–1, K), а также для некоторых классов специально конструируемых двоичных кодов. Близкие, но несколько худшие, свойства также проявляются у укороченных классов ЛБК.

Для всех кодов на основе М-последовательностей характерно следующее:

1) Количество частных оценок для всех входных переменных одинаково
2) Принятые кодовые элементы $y_1..y_7$ участвуют в формировании оценок одинаковое число раз т.е. вносят равный вклад в принятие окончательных решений, причём для каждого информационного элемента отдельно
3) Количество частных оценок чётное, что затрудняет мажоритарный принцип (в случае 50 / 50 – принять однозначное решение невозможно).

Следует, однако, учесть, что мажоритарное декодирование применимо не ко всем двоичным ЛБК. Во-первых, веса Хэмминга всех строк порождающей матрицы должны быть равны. Во-вторых, желательно, чтобы коды были систематическими, т.е. их порождающие матрицы перестановкой столбцов и строк приводились к виду **G**=(**E P**), где **E** – единичная подматрица прямого транспонирования информационных символов, **P** – подматрица формирования проверочных символов, имеющая особую структуру. Именно особая структура подматрицы **P** является третьим и определяющим требованием (необходимо отметить, что именно благодаря этому мажоритарное декодирование применимо и к некоторым несистематическим кодам). Очевидно, можно считать, что указанные требования должны предъявляться и недвоичным ЛБК.