

# Циклические коды

Выполнил:

Студент группы КТ-10-1

Золотаренко М.С.

- Код ,в котором кодовая комбинация, полученная путем циклического сдвига разрешенной кодовой комбинации является также разрешенной кодовой комбинацией называется циклическим (CRC - Cyclic Redundance Code) (полиномиальным, кодом с циклическими избыточными проверками-ЦИП).

- Циклический код относится к линейным, блочным, корректирующим, равномерным кодам.
- Сдвиг осуществляется справа налево, при этом крайний левый символ переносится в конец комбинации.
- В циклических кодах кодовые комбинации представляются в виде многочленов, что позволяет свести действия над кодовыми комбинациями к действию над многочленами (используя аппарат полиномиальной алгебры).

- Циклические коды являются разновидностью систематических кодов и поэтому обладают всеми их свойствами. Первоначально они были созданы для упрощения схем кодирования и декодирования. Их эффективность при обнаружении и исправлении ошибок обеспечила им широкое применение на практике.
- Циклические коды используются в ЭВМ при последовательной передаче данных

- Один из вариантов циклического кодирования заключается в умножении исходного кода на образующий полином  $g(x)$ , а декодирование - в делении на  $g(x)$ . Если остаток от деления не равен нулю, то произошла ошибка. Сигнал об ошибке поступает на передатчик, что вызывает повторную передачу.

- Операции кодирования и декодирования ЦК сводятся к известным процедурам умножения и деления полиномов. Для двоичных кодов эти операции легко реализуются технически с помощью линейных переключательных схем (ЛПС), при этом получаются относительно простые схемы кодеков, в чём состоит одно из практических достоинств ЦК.

- Циклические коды являются частным случаем систематических, линейных  $[n, k]$ -кодов. Название ЦК получили из-за своего основного свойства: циклическая перестановка символов разрешённой кодовой комбинации даёт также разрешённую кодовую комбинацию.
- Они высоконадёжны и могут применяться при блочной синхронизации, при которой выделение, например, бита нечётности было бы затруднительно.

- Если, например, A1 - 101100, то разрешённой кодовой комбинацией будет и A2 - 010110, полученная циклической перестановкой. Отметим, что перестановка производится вместе с проверочными символами, и по правилам линейных кодов сумма 6 по модулю 2 двух разрешённых кодовых комбинаций даёт также очередную разрешённую кодовую комбинацию.
- Описание ЦК связано с представлением кодовых комбинаций в виде полиномов (многочленов) фиктивной переменной "X". Для примера переведём

КС  $A_1 = 101100$  — полиномиальный вид

	6	5	4	3	2	1
Код	1	0	1	1	0	0

- При этом  $A_1(X) = 1 \cdot X^6 + 0 \cdot X^5 + 1 \cdot X^4 + 1 \cdot X^3 + 0 \cdot X^2 + 0 \cdot X^1 + 0 \cdot X^0 = X^6 + X^4 + X^3$ .



m	n	k	r	$g_n$	$G(X) \pmod 8$
3	7	4	3	1	13
4	15	11	4	1	23
		7	8	2	721
5	31	26	5	1	45
		21	10	2	3551
		16	15	3	107657
		11	20	5	5423325
6	63	57	6	1	103
		51	12	2	12471
		45	18	3	1701317
		39	24	4	166623567
		36	27	5	1033500423

m	n	k	r	$g_n$	$G(X) \pmod 8$
7	127	120	7	1	211
		113	14	2	41567
		106	21	3	11554743
		99	28	4	3447023271
		92	35	5	624730022327
8	255	247	8	1	435
		239	16	2	267543
		231	24	3	156720665
		223	32	4	75626641375
		215	40	5	23157564726421

## Ряд свойств, характеризующих корректирующую способность циклических кодов.

- Свойство 1. Циклический код с порождающим многочленом  $g(x)=1+x$  обнаруживает все ошибки нечетной кратности.
- Свойство 2. Циклический код с порождающим многочленом степени  $r=n-k$  обнаруживает любую пачку ошибок длиной  $r$  и менее.
- Свойство 3. Циклический код  $\frac{1}{2^{r-1}}$  не обнаруживает часть пачек ошибок длиной  $r$

-

- Рассмотрим процедуру кодирования по алгоритму:  

$$B_i(X) = A_i(X) \cdot X^r + R_i(X),$$
 где  $R_i(X)$  — остаток от деления  $A_i(X) \cdot X^r / G(X)$ .  
 $X^r$  - оператор сдвига  
 $A_i(X)$  –информационные и проверочные  $R_i(X)$  символы.
- В алгоритме можно выделить три этапа формирования кодовых комбинаций:
  - 1) к комбинации первичного кода  $A_i(X)$  дописывается справа  $r$  нулей, что эквивалентно умножению  $A_i(X)$  на  $X^r$  ;
  - 2) произведение  $A_i(X) \cdot X^r$  делится на соответствующий порождающий полином  $G(X)$  и определяется остаток  $R_i(X)$ , степень которого не превышает  $r - 1$ , этот остаток и даёт группу проверочных символов;
  - 3) вычисленный остаток присоединяется справа к  $A_i(X) \cdot X^r$ .

Пример 1. Рассмотрим процедуру кодирования по алгоритму (4.15): для кодовой комбинации  $A=1001$  сформировать кодовую комбинацию циклического кода (7,4).

В заданном ЦК  $n = 7, k = 4, r = 3$ , и из табл. 1 выберем порождающий полином  $G(X) = X^3 + X + 1$  (код Хемминга). Выполним три необходимые операции для получения кодовой комбинации ЦК согласно алгоритму (4.15):

$$A_i(X) = 1001 \sim X^3 + 1, \text{ (знак " } \sim \text{ " – тильда – означает соответствие).}$$

$$1. A_i(X) \cdot X^r = (X^3 + 1) \cdot X^3 = X^6 + X^3 \sim 1001000, \text{ ( } n=7\text{).}$$

$$2. A_i(X) \cdot X^r / G(X) = \begin{array}{r} X^6 + X^3 \\ + \\ X^6 + X^4 + X^3 \\ \hline X^4 \\ + \\ X^4 + X^2 + X \\ \hline X^2 + X \end{array} \left| \begin{array}{l} X^3 + X + 1 \\ \hline X^3 + X \end{array} \right.$$

- остаток  $R_i(X) = X^2 + X \sim 110$ .

$$3. B_i(X) = A_i(X) \cdot X^r + R_i(X) = 1001110 \text{ - итоговая комбинация ЦК.}$$

- Принятая кодовая комбинация ЦК (7,4) имеет вид  $V_i'(X)=1011110$ . Определить и исправить ошибку в  $V_i'(X)$ , если она имеется.
- Выполним три необходимые операции, проводимые при декодировании:

№ символа комбинации со старшего разряда	Ошибочный символ полинома комбинации	Синдром для порождающего полинома $G(X)=X^3+X+1$	Синдром для порождающего полинома $G(X)=X^3+X^2+1$	Шумовой вектор $z(X)$
7	$X^6$	101	110	1000000
6	$X^5$	111	011	0100000
5	$X^4$	110	111	0010000
4	$X^3$	011 = $H_k(7,4)$	101 = $\tilde{H}_k(7,4)$	0001000
3	$X^2$	100	100	0000100
2	$X^1$	010	010	0000010
1	$X^0$	001	001	0000001
		см. 4.29	см. 4.29	
	Нет ошибки	000	000	0000000

После передачи по каналу с помехами принимается кодовое слово

$$B_i'(X) = B_i(X) + z(X), \quad (4.16)$$

где  $B_i(X)$  - передаваемая кодовая комбинация;  $z(X)$  — полином (вектор) ошибки, имеющий степень от 1 до  $n-1$ .

При декодировании принятое кодовое слово делится на  $G(X)$

$$\frac{B_i'(X)}{G(X)} = U_i(X) + S_i(X), \quad (4.17)$$

где остаток от деления  $S_i(X)$  и является синдромом.

1) в соответствии с алгоритмом (4.17) производим

деление:

$$B_i'(X) / G(X) = X^6 + X^4 + X^3 + X^2 + X \quad \left| \begin{array}{l} X^3 + X + 1 \\ \hline X^3 \end{array} \right.$$

$$\underline{X^6 + X^4 + X^3}$$

$$X^2 + X \quad - \quad \text{остаток } R(X) = X^2 + X \sim 110,$$

отметим, что совпадение остатков в примере 1 и 2 — чисто случайное, в примере 1 остаток являлся проверочной группой кода, а в примере 2 - синдромом;

2) по полученному синдрому 110 в соответствующем опознавателе синдрома (дешифраторе синдрома, локаторе ошибки) определяем вид шумового вектора  $z(X)$  0010000 (см. табл. 2);

3) воспользовавшись алгоритмом (4.18), исправляем принятую кодовую комбинацию  $B_i'(X)$  и получаем переданную комбинацию  $B_i(X)$ :

$$B_i(X) = B_i'(X) + z(X) = \begin{array}{r} 1011110 \\ + \\ 0010000 \\ \hline 1001110 \end{array}$$

— исправленная комбинация на выходе