7 Циклічний код Хеммінга

Циклічні коди – це сімейство перешкодостійких код, що включає як один з різновидів коди Хеммінга. В цілому воно забезпечує велику гнучкість з погляду можливості реалізації код з необхідною здатністю виявлення і виправлення помилок, визначуваною параметром d0, в порівнянні з кодами Хеммінга (для яких d0=3 або d0=4). Широке використання циклічних код на практиці обумовлене також простотою реалізації відповідних кодерів і декодерів.

Основні властивості і само назва циклічних код пов'язані з тим, що всі дозволені комбінації битий в передаваному повідомленні (кодові слова) можуть бути отримані шляхом операції циклічного зрушення деякого початкового кодового слова:

(a0a1.$a_{n-2}a_{n-1}$);

(an-1a0a1.a_{n-2});

Циклічні коди задаються за допомогою так званих поліномів (многочленів) g(x) або їх коріння, що породжують. Поліном, що породжує, має вигляд

G(x)=g_r xr + gr-1 xr-1 + . + g0

де gi={0,1}, x=2. Крім того, вводяться поліном початкового повідомлення

u(x)= uk-1 xk-1 + uk-2 xk-2 + . +u_0

і кодованого повідомлення|сполучення|

A(x)= an-1 xn-1 + an-2 xn-2 + . + a0

Для цих поліномів, що є по суті альтернативним записом чисел в двійковій системі числення, визначаються операції складання, множення і ділення|поділки|, необхідні для організації кодування і декодування повідомлення|сполучення|. Всі операції виконуються по модулю 2.

Послідовність кодування на прикладі циклічної коди (7,4,3), мають g(x)= x3 + x + 1, наступна:

1) інформаційна частка|частина| повідомлення|сполучення| записується|занотовує| у вигляді полінома:

u(x)= uk-1 xk-1 + uk-2 xk-2 + . +u_0

У даному прикладі k=4 і для повідомлення 0111 виходить

u(x)= x2 + x + 1

2) u(x) умножається xr, що відповідає циклічному зрушенню початкового повідомлення на r розрядів вліво:

u(x) x3 = (x2 + x + 1) x3 = x5 + x4 + x3

3) отриманий многочлен ділиться на q(x):

u(x) •xr/q(x)= з(x) R(x) /q(x)

де з(x) – полином-частное з максимальним ступенем (k—1);

R(x) – поліном-залишок з максимальним ступенем (r-1);

– позначення порозрядної операції підсумовування по модулю 2 (що виключає АБО). Кодоване повідомлення представляється у вигляді

A(x)=u(x)xr R(x)

Таким чином, в цьому випадку

$$
\begin{array}{l|l}
\oplus\ x^5 + x^4 + x^3 & x^3 + x + 1 \\
\ x^5 + x^3 + x^2 & \hline x^2 + x = c(x) \\
\hline
\oplus\ x^4 + x^2 & \\
\ x^4 + x^2 + x & \\
\hline
\qquad\qquad x = R(x) &
\end{array}
$$

A(x)= (x5 + x4 + x3) x = x5 + x4 + x3 + x

Передаване кодоване повідомлення|сполучення| в звичайній|звичній| двійковій формі має вигляд|вид|

0111 010 - -до – битий r – битий

Один з можливих варіантів апаратурної реалізації кодера для даного прикладу змальований на рис. 10.4 разом з послідовністю сигналів, підтверджуючою отримання тих же перевірочних розрядів (010) на восьмому такті (r + до + 1=8). Кодером є сдвиговый регістр із зворотними зв'язками, організовуваними за допомогою елементів М2 (що виключає АБО, суматор по модулю 2). Структура зворотних зв'язків повністю визначається ненульовими коефіцієнтами полінома g(x), що породжує. На перших восьми тактах ключ Кл. знаходиться у верхньому положенні, формуються перевірочні розряди. Потім ключ Кл встановлюється в нижнє положення, що відповідає розриву ланцюгів зворотних зв'язків і передачі безпосередньо в канал зв'язку або на