

6. Код Файра

Найбільш відомим циклічним кодом, виконуючим поодинокі пачки помилок, являється код Файра, причому для цього потрібне невелике число перевірочних символів.

Утворюючий поліном даного коду $P(x) = q(x)(x^c + 1)$, де $q(x)$ - неприводимий многочлен ступеня t , що належить ступеня m ; c - просте число, яке не ділиться на m без залишку.

Многочлен $q(x)$ належить деякій мірі m , якщо m - найменше позитивне число таке, що двочлен $(x^m + 1)$ ділиться на $q(x)$ без залишку. Для будь-якого t існує, принаймні, один неприводимий многочлен $q(x)$ ступеня t , що належить показнику ступеня

$$m = 2t - 1$$

Наприклад, якщо $q(x) = x^3 + x^2 + 1$ ($t = 3$), то $m = 2t - 1 = 7$ і число c може набувати значень, які не діляться на сім, тобто 15, 16, 17, 18, 19, 20, 22, 23 і т.д.

Довжина коду Файра дорівнює найменшого спільного кратного чисел c і m тобто

$$n = \text{НОК}(c, m)$$

Число перевірочних інформаційних символів

$$k = n - c - t$$

Можна отримати код менший довжини з тим же числом перевірочних символів, якщо користуватися методом отримання укорочених циклічних кодів. При використанні кодів Файра можна виправити будь-яку одиночну пачку помилок довжини b або менше і одночасно виявити будь-яку пачку помилок довжини $l > b$ або менше, якщо $c > b + l - 1$ і $t > b$.

Якщо застосовувати ці коди тільки для виявлення помилок, можна виявити будь-яку комбінацію з двох пачок помилок, довжина найменшої з яких становить менше t , а сума довжин обох пачок не перевищує $(c + 1)$, а також будь-яку одиночну пачку помилок з довжиною, що не перевищує числа перевірочних символів $r = c + t$.