Построение кодов Рида-Маллера

Коды Рида – Маллера (РМ) являются двоичными групповыми кодами, эквивалентными циклическим кодам с добавленной общей проверкой на чётность по всем символам. Их относят к полиномиальным кодам наряду с такими кодами Боуза – Чоудхури – Хоквингема, Рида – Соломона и др. Они имеют большие кодовые расстояния и поэтому могут исправлять много ошибок. Очень выгодно их использование для каналов с малым отношением сигнал - шум. Так коды РМ длиной 32 символа использовались для передачи изображений Марса с борта космического корабля.

Коды Рида–Маллера нашли широкое применение в различных радиоэлектронных системах. Как правило, эти коды кодируются таким образом, что в результате получается неразделимый код. При этом используется однородная и регулярная структура порождающей матрицы G, позволяющая упростить декодирование кодов.

Параметры РМ-кодов:

$$n = 2^m;$$

$$k = 1 + C_m^1 + C_m^2 + \ldots + C_m^l;$$

$$r = n - k = 1 + C_m^1 + \ldots + C_m^{m-l-1};$$

$$d = 2^{m-l},$$

где n – длина кодового слова – количество символов, выбранных для передачи сообщения;

l– порядок кода;

$m \geq 3$;

k – число информационных символов;

r – число проверочных символов;

d – кодовое расстояние.

C_m^l - количество способов выбора из некоторого объёма m, математически оно определяется как:

$$C_m^l = \frac{m!}{l! \cdot (m - l)}.$$

Код Рида – Маллера порядка l определяется как код, базисом которого являются вектора $q_0, q_1, \dots, q_m$ и все векторные произведения из числа l или меньшего числа этих векторов.

В результате векторного произведения двух векторов результирующий вектор содержит произведения одноимённых компонентов. Если $a = (a_1, a_2, \dots, a_n)$, $b = (b_1, b_1, \dots, b_n)$, тогда результирующий вектор $c = (a_1b_1, a_2b_2, \dots, a_nb_n)$.

Коды Рида–Маллера первого порядка задаются порождающей матрицей G, первая строка которой состоит из единиц. В качестве столбцов остальных m строк используются все двоичные числа длиной m:

$$G_{PM-1} = \left[\begin{array}{cccccccccc} 1 & 1 & 1 & . & . & . & . & . & . & 1 \\ \hline 0 & 1 & 0 & 1 & . & . & . & . & . & 1 \\ 0 & 0 & 1 & 1 & . & . & . & . & . & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & . & . & . & 1 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & 0 & 0 & . & . & . & 1 \end{array}\right]. \quad \begin{array}{c} q_0 \\ q_1 \\ q_2 \\ q_3 \\ \\ q_m \end{array}$$

Например, при $m = 4$, $l = 1$ используется РМ-код первого порядка (РМ-1) с $n=2^4=16$, $k=5$, $d=2^3=8$.

$$G_{PM-1} = \left[\begin{array}{cccccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right. \quad \begin{array}{c} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \end{array}$$

Порождающая матрица РМ-кода второго порядка (РМ-2) состоит из порождающей матрицы G_{PM-1} и попарных произведений векторов (q_1, q_2, ... , q_m). Для РМ-2-кода длиной $n=16$ порождающая матрица будет содержать вектора- q_0, q_1,q_2,q_3,q_4, q_1q_2, q_1q_3, q_1q_4, q_2q_3, q_2q_4, q_3q_4. Параметры РМ-2 кода - $n=2^4=16$, $k=11$, $d=2^2=4$.

$$G_{PM-2} = \begin{bmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \end{bmatrix} \begin{matrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_1 q_2 \\ q_1 q_3 \\ q_1 q_4 \\ q_2 q_3 \\ q_2 q_4 \\ q_3 q_4 \end{matrix}$$

Порождающая матрица кода РМ-3 состоит из матрицы G_{PM-2} плюс все произведения по три вектора (q_1, q_2, ... , q_m) и т. д. Для РМ-3-кода длиной $n=16$ порождающая матрица будет содержать вектора- q_0, q_1,q_2,q_3,q_4, q_1q_2, q_1q_3, q_1q_4, q_2q_3, q_2q_4, q_3q_4, $q_1q_2q_3$, q_1,q_2,q_4, $q_1q_3q_4$, $q_2q_3q_4$. Параметры РМ-3 кода - $n=2^4=16$, $k=15$, $d=2^1=2$. Для РМ-

4-кода длиной $n=16$ порождающая матрица будет содержать вектора- q_0, q_1, q_2, q_3, q_4, q_1q_2, q_1q_3, q_1q_4, q_2q_3, q_2q_4, q_3q_4, $q_1q_2q_3$, q_1,q_2,q_4, $q_1q_3q_4$, $q_2q_3q_4$, $q_1q_2q_3q_4$. Параметры РМ-4 кода - $n=2^4=16$, $k=16$, $d=2^0=1$.

Кодирование информации РМ-кодами

Кодирование РМ-кодов осуществляется стандартным образом – путем умножения исходного вектора на порождающую матрицу:

$$a \times G = u.$$

Для РМ-1 кода длиной $n=2^3=8$ кодирование выполняется следующим образом:

$$u = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \end{bmatrix} \times \begin{array}{c} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \end{array} \begin{array}{l} q_0 \\ q_1 \\ q_2 \\ q_3 \end{array} , \qquad =$$

$$= \left[a_0, a_0 + a_3, a_0 + a_2, a_0 + a_2 + a_3, a_0 + a_1, a_0 + a_1 + a_3, a_0 + a_1 + a_2, a_0 + a_1 + a_2 + a_3 \right].$$

Очевидно, что при подобном кодировании образуется неразделимый код. Путем перестановки столбцов и суммирования строк можно привести порождающую матрицу G к приведенно-ступенчатому виду и, следовательно, получить разделимый код; однако при этом нарушается однородная структура кода.