Reed Mullerovy kódy

Jsou kódy umožňující vícenásobné opravy.

Jejich označení je RM(r,m), kde

- m určuje délku slov kódu, která je 2^m.
- r je řád kódu, kde $0 \leq r \leq m$.

Rekurzivní definice kódu

- $RM(0,m) = \{00...0, 11...1\}$ opakovací kód $(2^m,1)$
- $RM\{m,m\} = B^{2^m}$ všechna slova jsou kódová $(2^m,2^m)$
- $RM(r,m) = \{u(u+v) \mid u \in RM(r,m-1), v \in RM(r-1,m-1)\}$ pro $0<r<m$

Příklady.

RM(0,0) = {0, 1} opakovací kód (1,1)

RM(0,1) = {00, 11} opakovací kód (2,1)

RM(1,1) = {00, 01, 10, 11} kód (2,2)

RM(0,2) = {0000, 1111} opakovací kód (4,1)

RM(2,2) = {0000, 0001, 0010, 0011, 1000, 1001, 1010, …, 1111} kód (4,4)

RM(1,2) = {u(u+v)} u∈RM(1,1)={00, 01, 10, 11} v∈RM(0,1)={00, 11}

RM(1,2) = {u(u+00), u(u+11)}

RM(1,2) = {0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100}

Generující matice

G(r,m) nechť označuje generující matici kódu RM(r,m).

- $G(0,m) = (111...1)$ generující matice opakovacího kódu
- $G(r,m) = \begin{pmatrix} G(r,m-1) & G(r,m-1) \\ 0 & G(r-1,m-1) \end{pmatrix}$ 0 označuje nulovou submatici
- $G(m,m) = \begin{pmatrix} G(m-1,m) \\ 00..001 \end{pmatrix}$

Příklady.

$G(0,0) = (1)$

$G(0,1) = (1 \quad 1)$

$G(1,1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$G(0,2) = (1 \quad 1 \quad 1 \quad 1)$

$$G(1,2)=\begin{pmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$G(2,2)=\begin{pmatrix} G(1,2) \\ 0001 \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Příklad.

Kódování všech slov kódu RM(1,2) použitím generující matice G(1,2).

$$0000=(0\,0\,0)\begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{pmatrix} \quad 0101=(0\,1\,0)\begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{pmatrix} \quad 1010=(1\,1\,0)\begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{pmatrix}$$

$$1111=(1\,0\,0)\begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{pmatrix} \quad 0011=(0\,0\,1)\begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{pmatrix} \quad 0110=(0\,1\,1)\begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{pmatrix}$$

$$1001=(1\,1\,1)\begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{pmatrix} \quad 1100=(1\,0\,1)\begin{pmatrix} 1\,1\,1\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{pmatrix}$$

Vlastnosti kódu RM(r,m)

- Délka kódu: $n=2^m$.
- Minimální vzdálenost: $d=2^{m-r}$.
- Dimenze: $k=\sum_{i=0}^{r}\binom{m}{i}$
- RM(r-1,m) je obsažen v RM(r,m) pro r>0.

Lze ověřit matematickou indukcí.

Jiný způsob sestavení generující matice kódu RM(r,m)

Definujme vektory v_i

- pro i=0

  $v_0=(11\ldots1)$ 2^m hodnot 1

- pro $i=1..m$
  $v_i=(00…0\ 11…1\ 00…0\ 11…1\ \ …\ \ 00…0\ 11…1)$
  opakující se sekvence hodnot 0 a 1 délky 2^{i-1}

Příklad.

Pro $m=4$ máme vektory:

$v_0 = (1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1)$
$v_1 = (0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1)$
$v_2 = (0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1)$
$v_3 = (0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1)$
$v_4 = (0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1)$

Generující matice $G(r,m)$ je sestavena z vektoru v_0 a ze součinů 1 až r vektorů $v_1 \ldots v_m$.

Příklad.

Generující matici $G(2,4)$ sestavíme z vektoru v_0 a ze součinů 1 a 2 vektorů $v_1 \ldots v_3$:

$v_0 = (1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1)$
$v_1 = (0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1)$
$v_2 = (0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1)$
$v_3 = (0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1)$
$v_4 = (0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1)$
$v_1v_2 = (0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1)$
$v_1v_3 = (0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0\,1\,0\,1)$
$v_1v_4 = (0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1)$
$v_2v_3 = (0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,1\,1)$
$v_2v_4 = (0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1)$
$v_3v_4 = (0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1)$

$$k = 1 + \binom{4}{1} + \binom{4}{2} = 1 + 4 + 6 = 11$$

Kód (16,11) s minimální vzdáleností 4.

Příklad.

Pro generující matici $G(3,4)$ bychom ještě přidali součiny 3 vektorů:

$v_1v_2v_3 = (0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1)$
$v_1v_2v_4 = (0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1)$
$v_1v_3v_4 = (0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1)$
$v_2v_3v_4 = (0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1)$

a byl by to kód (16,15) s minimální vzdáleností 2 – kód sudé parity.

Příklad.

Generující matici $G(1,2)$ sestavíme z vektorů:

$v_0 = (1\,1\,1\,1)$
$v_1 = (0\,1\,0\,1)$
$v_2 = (0\,0\,1\,1)$

$$G(1,2) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Dekódování

Používá se metoda dekódování pro opakovací kód označovaná jako majoritní logické dekódování (majority logic decoding). Postup dekódování ukazuje následující příklad.

Dekódování pro kód RM(2,4)

Nechť kódovaná zpráva je

$a = a_0\, a_1\, a_2\, a_3\, a_4\, a_5\, a_6\, a_7\, a_8\, a_9\, a_{10}$.

Zakódované slovo je

$b = b_0\, b_1\, b_2\, b_3\, b_4\, b_5\, b_6\, b_7\, b_8\, b_9\, b_{10}\, b_{11}\, b_{13}\, b_{14}\, b_{15}$

$b = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_1v_2 + a_6v_1v_3 + a_7v_1v_4 + a_8v_2v_3 + a_9v_2v_4 + a_{10}v_3v_4$

Nechť přijaté slovo je

$c = c_0\, c_1\, c_2\, c_3\, c_4\, c_5\, c_6\, c_7\, c_8\, c_9\, c_{10}\, c_{11}\, c_{13}\, c_{14}\, c_{15}$.

$$G(2,4) = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}$$

Vypočítejme součty

$$\begin{aligned} b_0 + b_1 + b_2 + b_3 &= a_0 + a_0 + a_1 + a_0 + a_2 + a_0 + a_1 + a_2 + a_5 \\ &= 4a_0 + 2a_1 + 2a_2 + a_5 = a_5 \end{aligned}$$

$$\begin{aligned} b_4 + b_5 + b_6 + b_7 &= a_0 + a_3 + a_0 + a_1 + a_3 + a_6 + a_0 + a_2 + a_3 + a_8 + a_0 + a_1 + a_2 + a_3 + a_5 + a_6 + a_8 \\ &= 4a_0 + 2a_1 + 2a_2 + 4a_3 + a_5 + 2a_6 + 2a_8 = a_5 \end{aligned}$$

$$\begin{aligned} b_8 + b_9 + b_{10} + b_{11} &= \\ &= a_0 + a_4 + a_0 + a_1 + a_5 + a_4 + a_7 + a_0 + a_2 + a_4 + a_9 + a_0 + a_1 + a_2 + a_4 + a_5 + a_7 + a_9 \\ &= 4a_0 + 2a_1 + 2a_4 + a_5 + 2a_7 + 2a_9 = a_5 \end{aligned}$$

$$\begin{aligned} b_{12} + b_{13} + b_{14} + b_{15} &= \\ &= a_0 + a_1 + a_2 + a_{10} + a_0 + a_1 + a_3 + a_4 + a_6 + a_7 + a_{10} + a_0 + a_2 + a_3 + a_4 + a_8 + a_9 + a_{10} \\ &\quad + a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \\ &= 4a_0 + 2a_1 + 2a_2 + 4a_3 + 4a_4 + a_5 + 2a_6 + 2a_7 + 2a_8 + 2a_9 + 2a_{10} = a_5 \end{aligned}$$

Vypočítáme pro přijaté slovo c součty

$r_1 = c_0 + c_1 + c_2 + c_3$

$r_2 = c_4 + c_5 + c_6 + c_7$

$r_3 = c_8 + c_9 + c_{10} + c_{11}$

$r_4 = c_{12} + c_{13} + c_{14} + c_{15}$

a dekódujeme symbol a_5

$r_1 = r_2 = r_3 = r_4$	$a_5 = r_1$
$r_1 = r_2 = r_3 \quad r_4 \neq r_1$	$a_5 = r_1$
$r_1 = r_2 = r_4 \quad r_3 \neq r_1$	$a_5 = r_1$
$r_1 = r_3 = r_4 \quad r_2 \neq r_1$	$a_5 = r_1$
$r_2 = r_3 = r_4 \quad r_1 \neq r_2$	$a_5 = r_2$

V ostatních případech nelze symbol a_5 dekódovat - chybu nelze opravit.

Vypočítejme součty

$b_0 + b_1 + b_4 + b_5 = 4a_0 + 2a_1 + 2a_3 + a_6 = a_6$

$b_2 + b_3 + b_6 + b_7 = 4a_0 + 2a_1 + 4a_2 + 2a_3 + 2a_5 + a_6 + 2a_8 = a_6$

$b_8 + b_9 + b_{12} + b_{13} = 4a_0 + 2a_1 + 2a_3 + 4a_4 + a_6 + 2a_7 + 2a_{10} = a_6$

$b_{10} + b_{11} + b_{14} + b_{15} = 4a_0 + 2a_1 + 2a_2 + 2a_3 + 4a_4 + 2a_5 + a_6 + 2a_7 + 2a_8 + 4a_9 + 2a_{10} = a_6$

Z těchto vztahů vypočítáme

$r_1 = c_0 + c_1 + c_4 + c_5$

$r_2 = c_2 + c_3 + c_6 + c_7$

$r_3 = c_8 + c_9 + c_{12} + c_{13}$

$r_4 = c_{10} + c_{11} + c_{14} + c_{15}$

a dekódujeme symbol a_6 .

Tímto způsobem dekódujeme další symboly a_7, a_8, a_9, a_{10}.

Pokud se podaří všechny dekódovat (byla tam nejvýše jedna chyba, která byla opravena), vypočítáme nové d slovo z přijatého slova c a vypočítaných symbolů

$d = c - a_5v_1v_2 - a_6v_1v_3 - a_7v_1v_4 - a_8v_2v_3 - a_9v_2v_4 - a_{10}v_3v_4$.

Zřejmě pro slovo d platí

$d = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4$.

$$G(2,4)=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1\\0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1\\0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1\\0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1\\0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\end{pmatrix}$$

Z generující matice plyne

$d_0 + d_1 = 2a_0 + a_1 = a_1$

$d_2 + d_3 = 2a_0 + a_1 + 2a_2 = a_1$

$d_4 + d_5 = 2a_0 + a_1 + 2a_3 = a_1$

$d_6 + d_7 = 2a_0 + a_1 + 2a_2 + 2a_3 = a_1$

$d_8 + d_9 = 2a_0 + a_1 + 2a_4 = a_1$

$d_{10} + d_{11} = 2a_0 + a_1 + 2a_2 + 2a_4 = a_1$

$d_{12} + d_{13} = 2a_0 + a_1 + 2a_3 + 2a_4 = a_1$

$d_{14} + d_{15} = 2a_0 + a_1 + 2a_2 + 2a_3 + 2a_4 = a_1$

Vypočítáme

$r_1 = d_0 + d_1$

$r_2 = d_2 + d_3$

$r_3 = d_4 + d_5$

$r_4 = d_6 + d_7$

$r_5 = d_8 + d_9$

$r_6 = d_{10} + d_{11}$

$r_7 = d_{12} + d_{13}$

$r_8 = d_{14} + d_{15}$

a pokud se mezi hodnotami r_1 až r_8 některá vyskytuje vícekrát než druhá, lze dekódovat symbol a_1 .

Obdobně z generující matice plyne

$d_0 + d_2 = a_2$

$d_1 + d_3 = a_2$

$d_4 + d_6 = a_2$

$d_5 + d_7 = a_2$

$d_8 + d_{10} = a_2$

$d_9 + d_{11} = a_2$

$d_{12} + d_{14} = a_2$

$d_{13} + d_{15} = a_2$

a použitím těchto vztahů dekódujeme symbol a_2 .

Analogicky dekódujeme symboly a_3 a a_4 .

Pokud se tyto symboly podařilo dekódovat, vypočítáme další slovo

$e = d - a_1v_1 - a_2v_2 - a_3v_3 - a_4v_4$.

Zřejmě pro slovo e platí

$e = e_0\, e_1\, e_2\, e_3\, e_4\, e_5\, e_6\, e_7\, e_8\, e_9\, e_{10}\, e_{11}\, e_{13}\, e_{14}\, e_{15}$
$= a_0v_0 = a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0\, a_0$.

Pokud se mezi hodnotami e_0 až e_{15} některá vyskytuje vícekrát než druhá, lze dekódovat symbol a_0 .

Příklad.

Pro kód RM(1,3) sestavíme generující matici G(1,3) z vektorů:

$v_0 = (1\,1\,1\,1\,1\,1\,1\,1)$

$v_1 = (0\,1\,0\,1\,0\,1\,0\,1)$

$v_2 = (0\,0\,1\,1\,0\,0\,1\,1)$

$v_3 = (0\,0\,0\,0\,1\,1\,1\,1)$

$$G(1,3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Nechť kódovaná zpráva je

$a = 0010$.

Zakódované slovo je

$b = 00110011$.

Nechť přijaté slovo je

$c = 00100011$.

Z generující matice plyne

$b_0 + b_1 = a_1$

$b_2 + b_3 = a_1$

$b_4 + b_5 = a_1$

$b_6 + b_7 = a_1$

Vypočítáme

$c_0 + c_1 = 0$

$c_2 + c_3 = 1$

$c_4 + c_5 = 0$

$c_6 + c_7 = 0$

a dekódujeme $a_1 = 0$.

Z generující matice plyne

$b_0 + b_2 = a_2$

$b_2 + b_4 = a_2$

$b_4 + b_6 = a_2$

$b_5 + b_7 = a_2$

Vypočítáme pro $c = 00100011$

$c_0 + c_3 = 1$

$c_1 + c_3 = 0$

$c_4 + c_6 = 1$

$c_5 + c_7 = 1$

a dekódujeme $a_2 = 1$.

Z generující matice plyne

$b_0 + b_4 = a_3$

$b_1 + b_5 = a_3$

$b_2 + b_6 = a_3$

$b_3 + b_7 = a_3$

Vypočítáme pro $c = 00100011$

$c_0 + c_4 = 0$

$c_2 + c_5 = 0$

$c_2 + c_6 = 0$

$c_3 + c_7 = 1$

a dekódujeme $a_3 = 0$.

Vypočítáme další slovo

$d = c - a_1v_1 - a_2v_2 - a_3v_3 = 00100011 - 00110011 = 00010000$.

a dekódujeme $a_0 = 0$.

Dekódovaná zpráva je 0010 .