6 Reed-Mullerovy kódy

Buď F komutativní těleso. Polynomy v neznámých $x_1, \ldots, x_n$ tvoří okruh $F[x_1, \ldots, x_n]$. Každý takový polynom a lze zapsat jako

$$\sum a_{i_1,\ldots,i_m} x_1^{i_1} \ldots x_m^{i_m},$$

kde $i_1, \ldots, i_m$ jsou celá nezáporná čísla a kde $a_{i_1,\ldots,i_m} \in F$ je nenulové jen pro konečně mnoho m-tic $(i_1, \ldots, i_m)$. Maximum $i_1 + \cdots + i_m$ uvažované přes všechny m-tice, které splňují $a_{i_1,\ldots,i_m} \neq 0$, se nazývá *stupeň* polynomu a. Píšeme $\deg(a)$. Stupeň nulového polynomu definujeme jako -1. Polynomy $x_1^{i_1} \ldots x_m^{i_m}$ se nazývají *monomy*. (Terminologie zde kolísá. Často se za monom označuje i každý polynome $\lambda x_1^{i_1} \ldots x_m^{i_m}$, kde $\lambda \in F$ a $\lambda \neq 0$.)

Polynom nazveme *booleovský*, je-li $F = \mathbb{F}_2$ a současně $a_{i_1,\ldots,i_m} = 0$ kdykoliv $i_j \geq 2$ pro některé j, $1 \leq j \leq m$. Je-li $I = \{j_1, \ldots, j_r\} \subseteq \{1, \ldots, m\}$, tak monom $x_{j_1} \ldots x_{j_r}$ označíme zkráceně jako x_I. (Přitom $x_\emptyset = 1$.) Každý booleovský polynom v proměnných $x_1, \ldots, x_m$ lze tedy jednoznačně zapsat jako $\sum_{I \in \mathcal{M}} x_I$, kde $\mathcal{M}$ je nějaký systém podmnožin množiny $\{1, \ldots, m\}$.

Booleovské polynomy v proměnných $x_1, \ldots, x_n$ tvoří okruh, ve kterém $x_I \cdot x_J = x_{I \cup J}$. (Tento okruh je možno též získat faktorizací $\mathbb{F}_2[x_1, \ldots, x_m]$ přes ideál generovaný polynomy $x_i^2 - x_i$, $1 \leq i \leq m$.)

Booleovskou funkcí arity m se rozumí každé zobrazení $\mathbb{F}_2^m \to \mathbb{F}_2$. Každému polynomu $f \in \mathbb{F}_2[x_1, \ldots, x_m]$ můžeme přiřadit booleovskou funkci $\bar{f}$ arity m tak, že funkční hodnota v bodě $u = (u_1, \ldots, u_m)$ se spočítá dosazením u_i za x_i, $1 \leq i \leq m$ (je tedy rovna $f(u) = f(u_1, \ldots, u_m)$).

Booleovský polynom $a \in \mathbb{F}_2[x_1, \ldots, x_m]$ můžeme též psát jako $\sum a_I x_I$, kde I probíhá všechny podmnožiny $\{1, \ldots, m\}$ a kde $a_I \in \{0, 1\}$. Je-li $b = \sum b_J x_J \in \mathbb{F}_2[x_1, \ldots, x_m]$ také booleovský polynom, tak $a + b = \sum (a_I + b_I) x_I$ a $a \cdot b = \sum a_I b_J x_{I \cup J}$. Vidíme, že $ab(u_1, \ldots, u_m) = \sum a_I b_J x_{I \cup J}(u_1, \ldots, u_m) = \sum a_I x_I(u_1, \ldots, u_m) \cdot \sum b_J x_J(u_1, \ldots, u_m) = a(u_1, \ldots, u_m) \cdot b(u_1, \ldots, u_m)$. Tudíž $\overline{ab} = \bar{a} \cdot \bar{b}$, a podobně se snadno ověří, že $\overline{a + b} = \bar{a} + \bar{b}$. Zobrazení $a \to \bar{a}$ je tedy homomorfismem okruhů. Je-li $a = \sum a_I x_I$ nenulový booleovský polynom, tak vybereme $I \subseteq \{1, \ldots, m\}$ takové, aby $a_I = 1$ a současně aby bylo $|I|$ co nejmenší možné. Uvažme $u = (u_1, \ldots, u_m) \in \mathbb{F}_2^m$ tak, že $u_j = 1$ pokud $j \in I$ a $u_j = 0$ v ostatních případech. Je-li $J \subsetneq I$, tak $a_J = 0$. Je-li $I \setminus J \neq \emptyset$, pak $x_I(u) = 0$. Proto $a(u) = x_I(u) = 1$. Homomorfismus $a \to \bar{a}$ je tedy injektivní. Okruh booleovských polynomů má 2^{2^m} prvků, neboť je právě 2^m booleovských monomů. Okruh booleovských funkcí má také 2^{2^m} prvků, neboť $|\mathbb{F}_2^m| = 2^m$. Vidíme, že jde o izomorfismus a že platí

Tvrzení 6.1. *Každou booleovskou funkci arity m lze jednoznačně vyjádřit booleovským polynomem z $\mathbb{F}_2[x_1, \ldots, x_m]$.*

Toto tvrzení lze snadno dokázat i jinak. Je dobře známo, jak lze konstruovat booleovské funkce pomocí logických spojek AND a OR. Jestliže booleovské funkce f a g jsou realizovány booleovskými polynomy a a b (tedy $\bar{a} = f$ a $\bar{b} =$

g), tak booleovské funkce f AND g a f OR g jsou realizovány booleovskými polynomy $a \cdot b$ a $a + b + ab$. Protože každou booleovskou funkci lze vyjádřit jednoznačně pomocí disjunktivní normální formy (a samozřejmě také i pomocí konjuktivní normální formy), lze ji nutně vyjádřit i booleovským polynomem. Zápisu booleovské funkce f ve tvaru polynomu $\sum a_I x_I$, kde I probíhá všechny podmnožiny $\{1, \ldots, m\}$, se říká *algebraická normální forma*.

Prvku $(u_1, \ldots, u_m) \in \mathbb{F}_2^m$ budeme v dalším přiřazovat číselnou hodnotu $\sum u_i 2^{m-i}$. Tím jsou prvky přirozeně vzestupně uspořádány v lexikografickém pořadí $(0, \ldots, 0, 0)$, $(0, \ldots, 0, 1)$, $(0, \ldots, 1, 0)$, $(0, \ldots, 1, 1)$, $\ldots$, $(1, \ldots, 1, 1)$. Počítáme-li od nuly, tak j-tým prvkem je vektor, jehož souřadnice vyjadřují binární zápis čísla j. Incidenční vektor i_M, kde $M \subseteq \mathbb{F}_2^m$, budeme chápat vůči takovémuto pořadí.

Každé booleovské funkci f arity m přiřadíme vektor $v_f = (a_0, \ldots, a_{2^m-1})$, kde pro $j = \sum u_i 2^{m-i}$ máme $a_j = f(u_1, \ldots, u_m)$. Je-li $g \in \mathbb{F}_2[x_1, \ldots, x_m]$ booleovský polynom, tak $v_{\bar{g}}$ píšeme pouze jako v_g.

Připomeňme, že *afinním podprostorem* (ploskou) vektorového prostoru V se rozumí každá jeho podmnožina, kterou lze vyjádřit ve tvaru $a + U$, kde $a \in V$ a U je podprostor V.

Lemma 6.2. *Ať $I \subseteq \{1, \ldots, m\}$. Pak existuje afinní podprostor $A \subseteq \mathbb{F}_2^m$, který je kodimenze $r = |I|$, takový, že $v_{x_I} = i_A$.*

Důkaz Ať $I = \{i_1, \ldots, i_r\}$ a ať $v_{x_I} = (a_0, \ldots, a_{2^m-1})$. Pro $j = \sum u_i 2^{m-i}$ máme $a_j = 1$ právě když $u_{i_1} = u_{i_2} = \cdots = u_{i_r} = 1$. Proto je $(a_0, \ldots, a_{2^m-1})$ rovno i_A, kde $A = w + U$, přičemž $w = (1, \ldots, 1)$ je jedničkový vektor a U je vektorový podprostor tvořený všemi $(u_1, \ldots, u_m) \in \mathbb{F}_2^m$, které splňují $u_{i_1} = u_{i_2} = \cdots = u_{i_r} = 0$. Je zjevné, že $\dim A = \dim U = n - r$. □

Reed-Mullerův kód $\mathcal{R}(m, r)$ je binární kód délky 2^m tvořený právě všemi vektory v_a, kde a probíhá booleovské polynomy z $\mathbb{F}_2[x_1, \ldots, x_m]$, které jsou stupně nejvýše r.

Tvrzení 6.3. *Buď $0 \leq r \leq m$. Pak $\mathcal{R}(m, r)$ je lineární binární kód délky 2^m, dimenze $\binom{m}{0} + \cdots + \binom{m}{r}$ a minimální váhy 2^{m-r}.*

Důkaz. Booleovské polynomy stupně $\leq r$ tvoří vektorový podprostor prostoru všech booleovských polynomů v m proměnných. Označme ho na chvíli V_r. Za bázi V_r lze zvolit množinu všech booleovských monomů stupně $\leq r$, a proto $\dim V_r = \sum_{i \leq r} \binom{m}{i}$. Zobrazení $a \to v_a$ je izomorfismus V_r a $\mathcal{R}(r, m)$, takže tyto prostory mají stejnou dimenzi.

Podprostor $\mathbb{F}_2^m$ kodimenze r má 2^{m-r} prvků. Z Lemmatu 6.2 tudíž plyne, že $\mathcal{R}(m, r)$ obsahuje kódová slova váhy 2^{m-r}. Chceme ukázat, že $|v_a| \geq 2^{m-r}$ pro každé $a \in V_r$, $a \neq 0$. Jinými slovy, tvrdíme, že každé nenulové $a \in V_r$ nabývá hodnoty 1 alespoň v 2^{m-r} případech.

Je-li $r = 0$, tak V_r obsahuje pouze konstantní polynomy 0 a 1. Je-li $r = m$, tak se V_r skládá ze všech booleovských polynomů. V obou případech tvrzení zjevně

platí. Předpokládejme, že $m > r \geq 1$, a použijme indukci. Mějme $a = b + cx_m$, $a \neq 0$, kde $b, c \in \mathbb{F}_2[x_1, \ldots, x_{m-1}]$. Rozlišíme tři případy:

(1) $b \neq 0$ a $b+c \neq 0$. Máme $a(u_1, \ldots, u_{m-1}, 0) = b(u_1, \ldots, u_{m-1})$ a $a(u_1, \ldots, u_{m-1}, 1) = (b + c)(u_1, \ldots, u_{m-1})$. Podle indukčního předpokladu je $a(u_1, \ldots, u_m)$ nenulové v alespoň $2^{m-1-r} + 2^{m-1-r} = 2^{m-r}$ případech.

(2) $b = 0$ a $c \neq 0$. Jelikož c je stupně $\leq r - 1$, je $a(u_1, \ldots, u_{m-1}, 1) = c(u_1, \ldots, u_{m-1})$ nenulové v alespoň $2^{(m-1)-(r-1)} = 2^{m-r}$ případech.

(3) $b = c \neq 0$. I zde je $b = c$ stupně $\leq r - 1$, takže $a(u_1, \ldots, u_{m-1}, 0) = b(u_1, \ldots, u_{m-1}) \neq 0$ v alespoň $2^{(m-1)-(r-1)}$ případech.

□

Tvrzení 6.4. *Buď $0 \leq r \leq m$. Kód $\mathcal{R}(m, r)$ je generován množinou všech incidenčních vektorů i_A, kde $A \subseteq \mathbb{F}_2^m$ probíhá všechny afinní podprostory kodimenze r. Dále platí, že*

$$\mathcal{R}(m, r)^\perp = \mathcal{R}(m, m - r - 1).$$

Důkaz. Označme na chvíli $\mathcal{A}(m, r)$ lineární binární kód generovaný všemi i_A, kde kodimenze A je $\leq r$. Je-li B jiný afinní podprostor, řekněme kodimenze s, tak $A \cap B$ je buď množina prázdná, nebo je kodimenze nejvýše $r + s$. Přitom $r + s \leq m - 1$, pokud $s \leq m - 1 - r$. Je-li $r + s \leq m - 1$, je buď $A \cap B = \emptyset$, nebo $\dim(A \cap B) \geq 1$. Afinní prostory kladné dimenze mají v $\mathbb{F}_2^n$ sudý počet prvků. Proto z $r + s \leq m - 1$ plyne $i_A \cdot i_B = 0$, takže $\mathcal{A}(m, m - r - 1) \subseteq \mathcal{A}(m, r)^\perp$. Tudíž $\dim \mathcal{A}(m, m - r - 1) + \dim \mathcal{A}(m, r) \leq 2^m$.

Ukažme nyní, že $\mathcal{R}(m, r) \subseteq \mathcal{A}(m, r)$. Potřebujeme nahlédnout, že $x_I \in \mathcal{A}(m, r)$ pro každé $|I| \leq r$. Pro $|I| = r$ vztah plyne přímo z Lemmatu 6.2. Je-li $|I| = s < r$, tak podle téhož lemmatu je $x_I = i_B$, kde $\dim B = n - s > n - r$. Ovšem afinní podprostor B dimenze $n - s$ je zřejmě disjunktním sjednocením afinních podprostorů $A_1, \ldots, A_{2^{r-s}}$ dimenze $n - r \leq n - s$, takže $i_B = \sum i_{A_j}$, $1 \leq j \leq 2^{r-s}$.

Položme $\delta_r = \dim \mathcal{A}_{m,r} - \dim \mathcal{R}_{m,r}$. Podle Tvrzení 6.3 je $\dim \mathcal{R}(m, r) + \dim \mathcal{R}(m, m - r - 1) = \sum_{i=0}^{r} \binom{m}{i} + \sum_{j=0}^{m-r-1} \binom{m}{j}$. Z $\binom{m}{j} = \binom{m}{m-j}$ vyplývá, že tento součet je roven $\sum_{i=0}^{r} \binom{m}{i} + \sum_{i=r+1}^{m} \binom{m}{i} = \sum \binom{m}{i} = 2^m$. Máme tedy $\dim \mathcal{A}(m, m - r - 1) + \dim \mathcal{A}(m, r) = 2^m + \delta_r + \delta_{m-r-1} \leq 2^m$. Vidíme, že $\delta_r = 0$, takže $\mathcal{R}(m, r) = \mathcal{A}(m, r)$ a $\mathcal{R}(m, m - r - 1) = \mathcal{A}(m, m - r - 1) = \mathcal{R}(m, r)^\perp$. □

Geometrická interpretace Reed-Mullerových kódů umožňuje průhledný výklad a zdůvodnění tzv. *Reedova dekódovacího algoritmu* založeného na tzv. *většinové logice*. Budeme potřebovat

Lemma 6.5. *Ať $A \subseteq \mathbb{F}_2^m$ má méně než 2^a prvků a ať $s \geq 1$. Je-li $a + s \leq m$ a T je afinní podprostor dimenze $s - 1$, tak je parita $A \cap T$ shodná s převažující paritou $A \cap S$, kde S probíhá všechny afinní podprostory dimenze s. (Paritou množiny se rozumí informace o tom, zda počet jejích prvků je sudý nebo lichý.)*

Důkaz. Položme $b = m - s$ a zvolme afinní podprostor T dimenze $s - 1$. Pak T leží v $2^{b+1} - 1$ afinních podprostorech S dimenze s. Označme je S_i, kde $1 \leq i < 2^{b+1}$. Pro $1 \leq i < j < 2^{b+1}$ je $(S_i \setminus T) \cap (S_j \setminus T) = \emptyset$. Počet i takových, že $S_i \setminus T$ obsahuje prvek A, je tedy menší než $2^a \leq 2^b$. Je jich tedy nanejvýš $2^b - 1 < (2^{b+1} - 1)/2$. To znamená, že v nadpoloviční většině případů je $S_i \setminus T = \emptyset$. V těchto případech je parita S_i rovna T. Proto se parita T shoduje s převažující paritou S_i, $1 \leq i \leq 2^{b+1} - 1$. □

Důsledek 6.6. *Ať $A \subseteq \mathbb{F}_2^m$ má méně než 2^a prvků a ať $s \geq m - a$. Množina A je jednoznačně určena souborem parit všech množin $A \cap S$, kde S probíhá afinní podprostory dimenze s.*

Důkaz. Podle Lemmatu 6.5 lze zjistit paritu množin $A \cap S'$, kde S' probíhá afinní podprostory dimenze $s' = s - 1 < m - a$. Pro dané S' lze Lemma 6.5 použít na množinu $A' = A \cap S'$, a pak na $A \cap S'' = A' \cap S''$, kde S'' je dimenze $s - 2$, a tak dále, až se dostanemek k paritě $A \cap \{u\}$, $u \in \mathbb{F}_2^m$, neboť $\{u\}$ je afinní podprostor dimenze nula. Parita v tomto případě udává, zda prvek u do množiny A patří nebo ne. □

Uvažme nyní kód $\mathcal{R}(m, r)$, $1 \leq r \leq m-1$. Tento kód opravuje chyby, které jsou na méně než 2^{m-r-1} pozicích. Chybový vektor e, kde $|e| < 2^{m-r-1}$, je roven incidenčnímu vektoru i_E nějakého $E \subseteq \mathbb{F}_2^m$, $|E| < 2^{m-r-1}$. Podle Důsledku 6.6 pro určení E stačí znát parity $E \cap S$, kde S probíhá afinní množiny dimenze $r + 1$. Podle Tvrzení 6.4 v takovém případě i_S padne do $\mathcal{R}(m, r)^\perp$. Hodnotu $i_S \cdot i_E \equiv |S \cap E| \bmod 2$ ovšem známe, neboť $i_S \cdot e = i_S \cdot v$, kde v je přijaté slovo, ze kterého je chybový vektor e odvozen.

Z $i_S \cdot i_E$ tedy určíme $i_{S'} \cdot i_E$, kde S' je dimenze r, a tak dále, až získáme $i_{\{u\}} \cdot i_E = i_{\{u\} \cap E}$ pro každé $u \in \mathbb{F}_2^m$. Algoritmus lze mírně urychlit, jestliže pro S' uvážíme místo $\mathbb{F}_2^m$ nějakou nadrovinu, která S' obsahuje. Podobně pak i dále s klesající dimenzí S' lze zmenšit i dimenzi obalujícího podprostoru.