27.2.

1 Hammingovy perfektní kódy

1.1 Binární kódy

1.1. Označme $\mathcal{H}$ lineární kód s kontrolní maticí $H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

(a) Najděte generující matici kódu $\mathcal{H}$ ve standardním tvaru,

(b) určete vzdálenost kódu $\mathcal{H}$ a rozhodněte, zda je kód perfektní,

(c) rozhodněte, zda je $v = 1000101$ kódové slovo a případně které je nejbližší kódové slovo ke slovu v.

(a) Najdeme bázi $\mathrm{Ker} H_3 = \mathcal{H}$ a seřadíme ji do nějaké generující matice a tu upravíme pomocí Gaussovy-Jordanovy eliminace na odstupňovanou matici s kanonickými bázickými vektory (v této podobě ji můžeme rovnou hledat bázi):

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

(b) Stačí si všimnout, že žádný sloupec kontrolní matice H_3 není nulový ani není násobkem jiného sloupce, proto má kód vzdálenost aspoň 3. Naopak součet dokonce každých dvou sloupců je opět sloupcem matice, tedy náš kód má vzdálenost právě 3, a proto opraví právě jednu chybu.

Nyní snadno ověříme, že $1 + 7 = 2^{7-4}$, tedy se jedná o 1-perfektní kód.

4.3.

(c) Stačí spočítat $(Hv^T)^T = 011 \neq 000$, což znamená, že $v = 1000101$ kódové slovo není. Proto 3. sloupec kontrolní matice H obsahuje právě vektor Hv^T stačí změnit 3. souřadnici slova v na slovo $c = 1010101$, aby $(Hc^T)^T = 000$. □

Pro $l \in \mathbb{N}$ seřaďme všechna nenulová slova množiny $\mathbb{F}_2^l$ do sloupců H_l, položme $n := 2^l - 1$ a definujme lineární kód $\mathcal{H}_l := \{c \in \mathbb{F}_2^n \mid Hc^T = 0^T\}$.

1.2. Pro $l \in \mathbb{N}$

(a) ověřte, že je H_l kontrolní matice kódu $\mathcal{H}_l$,

(b) určete vzdálenost a dimenzi $\mathcal{H}_l$ a rozhodněte, zda je kód perfektní,

(c) navrhněte algoritmus, jak opravit jednu chybu přijatého slova.

(a) Stačí si všimnout, že ve sloupcích matice H_l máme kanonickou bázi vektorového prostoru $\mathbb{F}_2^l$, a tudíž má hodnost rovnu počtu řádků.

(b) Provedeme-li stejnou úvahu jako v bodu (c) předchozí úlohy, vidíme, že vzdálenost kódu je 3, jedná se tedy o $[2^l-1, 2^l-l-1, 3]_2$-kód, který opravuje 1 chybu. Snadno tedy zjistíme, že levá strana Hammingovy nerovnosti je rovna $1 + 2^l - 1 = 2^l$ a pravá strana má hodnotu $2^{2^l-1-(2^l-l-1)} = 2^l$. To znamená, že $\mathcal{H}_l$ je o 1-perfektní kód.

(c) Kód je 1-perfektní, tedy pro každé nekódové slovo existuje ve vzdálenosti 1 právě jedno kódové slovo. Nechť v je přijaté slovo. Pokud $H_l v^T = \mathbf{0}^T$, pak $v \in \mathcal{H}_l$. Pokud $H_l v^T \neq \mathbf{0}^T$, pak existuje i, pro než je $H_l v^T$ právě i-tým sloupcem. Nyní stačí vzít slovo $c = v + e_i$, pro něž platí, že $d(v, c) = 1$ a

$$cH_l^T = (v + e_i)H_l^T = vH_l^T + h_i = h_i + h_i = \mathbf{0}$$

tedy $c \in \mathcal{H}_l$ je opravené slovo.

Označíme-li $\alpha : \mathbb{F}_2^l \setminus \{0\} \to \{1, \ldots, 2^l - 1\}$ zobrazení dané předpisem $\alpha(c_1 \ldots c_l) = \sum_{i=1}^{l} c_i 2^{i-1}$, tj. $\alpha^{-1}(i)$ je právě binární zápis hodnoty $i \in \{1, \ldots, 2^l - 1\}$ (doplněný nulami). Předpokládejme, že v i-tém sloupci matice H_l je právě $\alpha^{-1}(i)^T$. Potom každé slovo $c \in \mathbb{F}_2^l \setminus \mathcal{H}_l$ platí, že $c + e_{\alpha(cH^T)} \in \mathcal{H}_l$. □

1.2 q-ární kódy

1.3. Nad konečným tělesem $\mathbb{F}_q$ sestrojte obdobným způsobem jako v předchozí úloze kontrolní matici perfektního kódu délky $n := \frac{q^l-1}{q-1} = \sum_{i=0}^{l-1} q^i$ dimenze $n - l$. Jaká je jeho Hammingova vzdálenost?

Vezmeme množinu všech přímek (tj. projektivní prostor) ve vektorovém prostoru dimenze l, kterých je právě $n := \frac{q^l-1}{q-1} = \sum_{i=0}^{l-1} q^i$ a z každé přímky vezmeme jeden nenulový vektor h_i. Tyto vektory sestavíme do matice M typu $l \times n$, která je jistě hodnosti l. Každé dva sloupce jsou přitom lineárně nezávislé, neboť neleží na stejné přímce, ale každá dvojice určuje rovinu, která obsahuje jiný sloupcový vektor, proto je vzdálenost kódu 3. Máme tedy $[n, n - l, 3]_q$-kód.

Zbývá zjistit, že levá strana Hammingovy nerovnosti je $1 + n(q - 1) = 1 + \frac{q^l-1}{q-1}(q - 1) = q^l$, zatímco pravá strana je $q^{n-(n-l)} = q^l$, tudíž je kód opět 1-perfektní. □

1.4. Nad konečným tělesem $\mathbb{F}_q$ spočítejte velikost koule $V_q(n,r)$.

Nejprve spočítáme velikost množiny A_i všech slov váhy i:

$$|A_i| = |\{c \in \mathbb{F}_q^n |\ w(c) = n\}| = |\{I \subseteq \{1,\dots n\} | I| = i\}| \cdot |(\mathbb{F}_q^*)^i| = \binom{n}{i}(q-1)^i.$$

Potom dostáváme $V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$ □

13.3.

2 Samoduální kódy

2.1. Určete všechny prametry a rozhodněte, zda je samoduální lineární kód nad $\mathbb{F}_3$ s generující maticí

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

Protože je C hodnosti 4, jedná se o kód délky 8 a dimenze 4. Snadno spočítáme, že $CC^T = \mathbf{0}$, proto C generuje samoduální lineární kód. To znamená, že C je kontrolní matice kódu a z ní snadno zjistíme, že žádné dva sloupce nejsou lineárně nezávislé, zatímco tři sloupce už jsou lineárně závislé. Proto má kód vzdálenost 3. Jeho parametry tedy jsou $[8,4,3]_3$. □

2.2. Dokažte, že neexistuje samoduální lineární kód s parametry $[6,3]_3$.

Předpokládejme, že takový kód exsituje, tedy musí podle věty z přednášky existovat nějaký samoduální lineární kód s parametry $[6,3]_3$ s generující maticí ve standardním tvaru $(I_3|A)$, kde $A \in \mathbb{F}_3^{3\times 3}$. Protože jde o samoduální kód musí platit

$$\mathbf{0} = (I_3|A)(I_3|A)^T = I_3 + AA^T,$$

a proto $AA^T = -I_3$. Protože

$$-1 = \det(-I_3) = \det(AA^T) = (\det A)^2.$$

dostáváme spor s vlastostí tělesa $\mathbb{F}_3$ v němž $a^2 \neq -1$ pro žádné $a \in \mathbb{F}_3$. □

2.3. Dokažte, že matice ve standardním tvaru $(I_k|A)$, kde $A \in \mathbb{F}_q^{k\times k}$ je maticí samoduálního kódu, právě když $AA^T = -I_k$.

Stačí zopakovat úvahu předchozí úlohy podle níž je lineární kód generovaný maticí $(I_k|A)$ samoduální , právě když

$$\mathbf{0} = (I_k|A)(I_k|A)^T = I_k + AA^T \Leftrightarrow AA^T = -I_k$$

□

2.4. Najděte nějaký samoduální kód délky 14 a 16 nad tělesem $\mathbb{F}_5$ vzdálenosti aspoň 3.

Protože v $\mathbb{F}_5$ platí, že $2^2 = 3^2 = -1$ snadno nahlédneme, že matice $(I_k|2I_k)$ generuje lineární samoduální kód s parametry $[2k, k, 2]_5$ pro každé k. Ten ovšem nesplňuje požadavek na vzdálenost. S využitím předchozí charakterizace najdeme matici A, aby $AA^T = -I_k$ pro $k = 7, 8$. Generující (a zároveň kontrolní) matice samoduálních kódů jsou například matice $(I_7|A_7)$ a $(I_8|A_8)$ pro

$$A_7 = \begin{pmatrix} 0 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 0 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 0 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 0 \end{pmatrix}, \quad A_8 = \begin{pmatrix} 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 4 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 4 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 4 \end{pmatrix}.$$

Vzdálenost obou kódů je 4. □

3 Cyklické kódy

Připomeňme, že kód $\mathcal{C} \subseteq \mathbb{F}_q^n$ je *cyklický*, jestliže

$$c_0c_1 \dots c_{n-2}c_{n-1} \in \mathcal{C} \Rightarrow c_{n-1}c_0 \dots c_{n-3}c_{n-2} \in \mathcal{C}.$$

Symbolem $\mathbb{F}_q[x]_n$ označíme $\mathbb{F}_q$-algebru (tedy vektorový prostor nad $\mathbb{F}_q$ se strukturou okruhu) s nosnou množinou $\mathbb{F}_q^n$, operacemi $+, -$ aritmetického vektorového prostoru. Násobení je určeno vztahem

$$0a0 \dots 0 \cdot c_0c_1 \dots c_{n-2}c_{n-1} = c_0c_1 \dots c_{n-2}c_{n-1} \cdot 0a0 \dots 0 = a \cdot c_{n-1}c_0 \dots c_{n-3}c_{n-2},$$

kde násobení vpravo je násobení skalárem a na aritmetickém vektorovém prostoru $\mathbb{F}_q^n$. Je snadné si uvědomit, že násobení je tímto vztahem a distributivitou jednoznačně určeno, tak aby $\mathbb{F}_q[x]_n$ byl komutativní okruh s jednotkou $\mathbf{1} = 10 \dots 00$.

Definujme $\nu : \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n-1)$ vztahem

$$\nu(c_0c_1\dots c_{n-2}c_{n-1}) = [\sum_{i=0}^{n-1} c_i x^i],$$

kde hranaté závorky vpravo označují rozkladovou třídu faktorového okruhu $\mathbb{F}_q[x]/(x^n-1)$ modulo hlavní ideál (x^n-1).

3.1. Dokažte, že ν představuje izomorfismus okruhů $\mathbb{F}_q[x]_n$ a $\mathbb{F}_q[x]/(x^n-1)$.

Nejprve si uvědomíme, že pro každé dva polynomy $p, q \in F_q[x]$ se shodují jim příslušné rozkaldové třídy

$$[p] = p+(x^n-1) = \{p+a\cdot(x^n-1)|\ a \in F_q[x]\} = \{q+a\cdot(x^n-1)|\ a \in F_q[x]\} = q+(x^n-1) = [q],$$

právě když $p \equiv q(\mathrm{mod} x^n-1)$, což platí, právě když $p-q \in (x^n-1)$. Proto $([p]) = ([(p)\mathrm{mod} x^n-1])$. Odtud dostáváme jednak

(a) že $[p] = [(p)\mathrm{mod} x^n-1]$, tedy pro $\nu(c_0c_1\dots c_{n-2}c_{n-1}) = [p]$ pro $\sum_{i=0}^{n-1} c_i x^i = (p)\mathrm{mod} x^n-1$ a ν je na

(b) a dále že pokud $\nu(\cdot c_0c_1\dots c_{n-2}c_{n-1}) = [0]$, pak x^n-1 dělí $\sum_{i=0}^{n-1} c_i x^i$, proto $c_0c_1\dots c_{n-2}c_{n-1} = \mathbf{0}$ a tedy ν je prosté.

Z definice vidíme, že zobrazení ν je lineární zobrazení a protože

$$\nu(0a0\dots00)\cdot\nu(c_0c_1\dots c_{n-2}c_{n-1}) = [ax]\cdot[\sum_{i=0}^{n-1} c_i x^i] = [\sum_{i=0}^{n-1} ac_i x^{i+1}] =$$

$$= [ac_{n-1}x^0 + \sum_{i=0}^{n-2} ac_i x^i] = \nu(0a0\dots0\cdot c_0c_1\dots c_{n-2}c_{n-1}).$$

zobrazení ν je okruhový homomorfismus. □

3.2. Dokažte, že lineární kód $\mathcal{C} \subseteq \mathbb{F}_q^n$ je cyklický, právě když jde o ideál okruhu $\mathbb{F}_q[x]_n$.

Protože ν je izomorfismus, stačí dokázat, že $\mathcal{C} \subseteq \mathbb{F}_q^n$ je cyklický lineární kód, právě když $\nu(\mathcal{C})$ je ideál okruhu $\mathbb{F}_q[x]/(x^n-1)$.

Nechť $\mathcal{C}$ je cyklický lineární kód. Protože je $\mathcal{C}$ lineární, je $\nu(\mathcal{C})$ je podprostor $\mathbb{F}_q$-vektorového prostoru $\mathbb{F}_q[x]/(x^n-1)$ Protože je $\mathcal{C}$ uzavřeno na cyklické posunutí, tj. na $\nu(\mathcal{C})$ je uzavřeno na násobení monomem $[x]$, indukcí zjistíme,

že pro každé $i \leq 1$ a $[p] \in \nu(\mathcal{C})$ platí, že $[x^i] \cdot [p] = [x] \cdot [x^{i-1}] \cdot [p] \in \nu(\mathcal{C})$, a proto pro každé $\sum_i a_i x^i \in \mathbb{F}_q[x]$

$$[\sum_i a_i x^i] \cdot [p] = \sum_i a_i [x^i \cdot p] \in \nu(\mathcal{C}).$$

Je-li naopak $\nu(\mathcal{C})$ ideál okruhu $\mathbb{F}_q[x]/(x^n - 1)$, pak $\mathcal{C}$ je lineární kód, protože ν je izomorfismus vektorových prostorů a $\nu(\mathcal{C})$ podprostor. Podmínka cykličnosti plyne z uzavřenosti $\nu(\mathcal{C})$ na násobení prvkem $[x]$. □

Připomeňme, že $\mathbb{F}_q[x]$ i $\mathbb{F}_q[x]/(x^n-1)$ jsou okruhy hlavních ideálů. Protože $([a]) = ([\mathrm{NSD}(a, x^n - 1)])$, jsou ideály $\mathbb{F}_q[x]/(x^n - 1)$ právě tvaru $([f])$ pro taková f, která dělí polynom $x^n - 1$.

Pro libovolné $f/x^n - 1$ definujme množinu

$$\mathcal{C}(f) := \{c_0 c_1 \dots c_{n-1} \in \mathbb{F}_q^n | \ \exists g \in \mathbb{F}_q[x] : \deg g < n - \deg f, \sum_i c_x^i = g \cdot f\}.$$

3.3. Dokažte, že lineární kód $\mathcal{C} \subseteq \mathbb{F}_q^n$ je cyklický, právě když existuje polynom $f \in \mathbb{F}_q[x]$, pro který $f/x^n - 1$.

Díky předchozím úlohám a charakterizaci ideálů okruhu $\mathbb{F}_q[x]/(x^n - 1)$ stačí ověřit, že pro každé $f/x^n - 1$ je $\nu(\mathcal{C}) = ([f])$. Z definice $\mathcal{C}(f)$ přitom platí, že $\nu(\mathcal{C}) \subseteq ([f])$. Naopak nechť $[h] \in ([f])$ a označme $g := \frac{x^n-1}{f}$. Potom existuje $a \in \mathbb{F}_q[x]$, pro které

$$[h] = [a] \cdot [f] = [(af) \mathrm{mod} x^n - 1] = [(a) \mathrm{mod} g \cdot f] \in \nu(\mathcal{C}),$$

tedy $([f]) \subseteq \nu(\mathcal{C})$. □

18.3.

Nechť pro $f = \sum_i f_i x^i, g = \sum_i g_i x^i \in \mathbb{F}_q[x]$ platí, že $x^n - 1 = f \cdot g$ a označme $k := \deg g$ a $m := \deg f = n - k$. Připomeňme, že generující matici kódu $\mathcal{C}(f)$ lze zapsat ve tvaru

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_m & 0 & 0 & \dots & 0 & 0 \\ 0 & g_0 & \dots & g_{m-1} & g_m & 0 & \dots & 0 & 0 \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \dots & \cdot & \cdot \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \dots & \cdot & \cdot \\ 0 & 0 & \dots & \cdot & \cdot & \dots & \dots & g_m & 0 \\ 0 & 0 & \dots & \cdot & \cdot & \dots & \dots & g_{m-1} & g_m \end{pmatrix} \in \mathbb{F}_q^{k \times n}$$

a kontrolní matici kódu $\mathcal{C}(f)$ lze zapsat ve tvaru $H \in \mathbb{F}_q^{m\times n}$

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 & 0 \\ 0 & h_k & \dots & h_1 & h_0 & 0 & \dots & 0 & 0 \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \dots & \cdot & \cdot \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \dots & \cdot & \cdot \\ 0 & 0 & \dots & \cdot & \cdot & \dots & \dots & h_0 & 0 \\ 0 & 0 & \dots & \cdot & \cdot & \dots & \dots & h_1 & h_0 \end{pmatrix} \in \mathbb{F}_q^{m\times n}.$$

3.4. Najděte všechny binární lineární cyklické kódy délky 5, víte-li, že

$$x^5 - 1 = (x+1)(1+x+x^2+x^3+x^4)$$

je ireducibilní rozklad v $\mathbb{F}_2[x]$. Pro netriviální určete jejich generující a kontrolní matici a jejich parametry.

Snadno určíme všechny dělitele $x^5 - 1$ a najdeme čtyři kódy:

$$\mathcal{C}(1) = \mathbb{F}_2^5, \quad \mathcal{C}(x^5-1) = \mathbf{0}, \quad \mathcal{C}(x+1), \quad \mathcal{C}(\sum_{i=0}^{4} x^i).$$

Označíme-li

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

pak A tvoří generující matici kódu $\mathcal{C}(x+1)$ a kontrolní matici kódu $\mathcal{C}(\sum_{i=0}^{4} x^i)$ a B tvoří kontrolní matici kódu $\mathcal{C}(x+1)$ a generující matici kódu $\mathcal{C}(\sum_{i=0}^{4} x^i)$. Z kontrolních matice snadno určíme vzdálenost kódů, proto je $\mathcal{C}(x+1)$ $[5,4,2]_2$-kód a $\mathcal{C}(\sum_{i=0}^{4} x^i)$ je $[5,1,5]_2$-kód □

3.5. Nechť známe ireducibilní rozklad $x^7-1 = (x+1)(x^3+x+1)(x^3+x^2+1)$ v oboru $\mathbb{Z}_2[x]$.

(a) Najděte generující a kontrolní matici kódu $\mathcal{C}(x^3+x+1)$.

(b) Kolik různých binárních cyklických kódů délky 7 existuje?

(c) Ověřte, že je kód $\mathcal{H}$ z úlohy 1.1 permutačně ekvivalentní s kódy $\mathcal{C}(x^3+x+1)$ a $\mathcal{C}(x^3+x^2+1)$.

(a) Okamžitě ze znalosti koeficientů polynomu $x^3 + x + 1$ dostáváme generující matici

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Pro kontrolní matici nám stačí spočítat $(x+1)(x^3+x^2+1) = x^4+x^2+x+1$ a kontrolní matici tedy dostaneme obdobnou konstrukcí

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

(b) Různých binárních cyklických kódů délky 7 máme právě tolik kolik je (neasociovaných) dělitelů polynomu f, tedy

$$|\{(x+1)^{i_1}(x^3+x+1)^{i_2}(x^3+x^2+1)^{i_3} |\ i_1, i_2, i_3 \in \mathbb{Z}_2\}| = 8.$$

(c) Nejprve stejně jako v úloze (a) spočítáme kontrolní matici cyklického kódu $\mathcal{C}(x^3+x^2+1)$. Protože $\frac{x^7-1}{x^3+x^2+1} = (x+1)(x^3+x+1) = x^4+x^3+x^2+1$, dostáváme

$$K = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

kontrolní matici kódu $\mathcal{C}(x^3 + x^2 + 1)$. Protože právě permutace $(246)(35)$ sloupců převede matici K na matici H, jedná se o permutaci zprostředkující permutační ekvivalenci kódů $\mathcal{C}(x^3 + x^2 + 1)$ a $\mathcal{C}(x^3 + x + 1)$. □

3.6. Rozhodněte, pro která i existuje nějaký cyklický $[10, i]_3$ kód, víme-li, že ireducibilní rozklad polynomu $x^{10} - 1 \in \mathbb{Z}_3[x]$ je tvaru $(x-1)(x+1)Q_5Q_{10}$, kde Q_5 a Q_{10} jsou ireducibilní (cyklotomické) polynomy stupně 4.

Z ireducibilního rozkladu vidíme, že dělitelé polynomu $x^{10} - 1$ jsou v $\mathbb{Z}_3[x]$ právě stupně $0, 1, 2, 4, 5, 6, 8, 9, 10$. Protože každý cyklický kód je tvaru $\mathcal{C}(f)$ pro nějaké polynomy g, h splňující $x^{10} - 1 = gh$ a $\dim \mathcal{C}(f) = n - \deg f = \deg g$, existují ternární lineární cyklický kód déky 10 a dimenze $i = 0, 1, \ldots, 10$ s výjimkou dimeneze 3 a 7. □

4 GRS a BCH kódy

4.1 Kontrolní matice GRS-kódu

4.1. Nechť $\alpha_1, \ldots, \alpha_n$ jsou po dvou různé prvky tělesa $\mathbb{F}_q$ a $k < n$. Ukažte, že je matice $G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \cdot & \cdot & \ldots & \cdot \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix}$ generující maticí GRS-kódu s lokátory $\alpha_1, \ldots, \alpha_n$. Jak spočítat jeho multiplikátory?

Položme

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \cdot & \cdot & \ldots & \cdot \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \ldots & \alpha_n^{n-k-1} \end{pmatrix}.$$

Hledáme takový vektor $\mathbf{x} = x_1 \ldots x_n \in (\mathbb{F}_q^*)^n$, že

$$0 = G(H\mathbf{x})^T = G\mathbf{x}^T H^T.$$

Prostým roznásobením zjistíme, že počítáme řešení soustavy rovnic

$$\sum_{i=1}^{n} x_i \alpha_i^j \quad j = 0, \ldots n-k-2.$$

Matice této soustavy má tvar $\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \cdot & \cdot & \ldots & \cdot \\ \alpha_1^{n-k-2} & \alpha_2^{n-k-2} & \ldots & \alpha_n^{n-k-2} \end{pmatrix}$, je typu $n-1 \times n$ a každá matice, která z ní vznikne vypuštěním jednoho sloupce je regulární čtvercovou Vandermondtovou maticí stupně $n-1$. To znamená, že libovolná netriviální lineární kombinaci méně než n sloupů matice je nenulový vektor, neboť jsou lineárně nezávislé. Proto existuje netriviální řešení a jeho všechny souřadnice jsou nutně nenulové. □

25.3.

4.2 Konstrukce GRS a RS kódů

4.2. Najděte MDS kód s parametry $[n, k, d]$

(a) pro daná $0 < k < n$,

(b) pro daná $0 < d < n$,

(c) pro daná $0 < d, k$.

Ve všech případech využijeme vztahu $d = n - k + 1$ a konstrukce GRS-kódu.

(a), (b) zvolíme těleso $\mathbb{F}_q$ pro $q > n$ a a jeho po dvou různé prvky $\alpha_1, \ldots, \alpha_n$.

(c) Položíme $n = k + d - 1$ a pokračujeme jako v (a)

Nyní je $H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \cdot & \cdot & \ldots & \cdot \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \ldots & \alpha_n^{n-k-1} \end{pmatrix}$ kontrolní matice hledaného kódu. □

4.3. Najděte generující a kontrolní matici nějakého MDS kódu s parametry $[5, 3, 3]$ a $[5, 2, 4]$

Zvolíme například těleso $\mathbb{F}_7$.

Pak je matice $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ kontrolní maticí GRS kódu s parametry $[5, 3, 3]_7$ a generující maticí GRS kódu s parametry $[5, 2, 4]_7$.

Snadno dopočítáme, že například matice $G = \begin{pmatrix} 1 & 5 & 1 & 0 & 0 \\ 2 & 4 & 0 & 1 & 0 \\ 3 & 3 & 0 & 0 & 1 \end{pmatrix}$ je odpovídající generující matice GRS kódu s parametry $[5, 2, 4]_7$ a kontrolní matice GRS kódu s parametry $[5, 3, 3]_7$. □

4.4. Najděte RS-kód s parametry (a) $[5, 3, 3]_q$, (b) $[7, 5, 3]_q$, (c) $[7, 4, 4]_q$.

(a) Hledáme q, pro které 5 dělí $q - 1$. Víme, že q musí být mocninou prvočísla a snadno tedy nahlédneme, že nejmenší přípustné $q = 11$. Nyní musíme zvolit prvek řádu 5 v $\mathbb{F}_{11}$. Protože $2^5 = -1$ v $\mathbb{F}_{11}$, vidíme, že vyhovuje například prvek 4, tedy kontrolní matice RS $[5, 3, 3]_{11}$ je tvaru $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 5 & 9 & 3 \end{pmatrix}$.

(b) Tentokrát hledáme q, pro které 7 dělí $q-1$, zřejmě je to právě $q = 2^3$. Reprezentujme si prvky tělesa $\mathbb{F}_8$ pomocí kořenu α polynomu $x^3 + x + 1$ ireducibilního nad $\mathbb{F}_2$, tedy $\mathbb{F}_8 = \mathbb{F}_2[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{F}_2\}$. Protože

je grupa $\mathbb{F}_8^*$ cyklická, je každý nejednotkový prvek řádu 7. Nyní dopočítáme, že například matice

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha+1 & \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^2+1 \end{pmatrix}.$$

je kontrolní maticí RS $[7,5,3]_8$-kódu

(c) Postupujeme stejně jako v (b) a dostáváme nejmenší $q = 8$ a kontrolní matici $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha+1 & \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^2+1 \\ 1 & \alpha^2 & \alpha^2+\alpha & \alpha^2+1 & \alpha & \alpha^2+1 & \alpha^2+\alpha+1 \end{pmatrix}$. □

4.3 Konstrukce BCH kódů

4.5. Najděte kontrolní matici a určete parametry binárního BCH-kódu určeného RS kódem s parametry $[7,5,3]_8$.

Budeme pracovat se stejnou prezentací $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ pro $\alpha^3+\alpha+1$. Hledáme binární slova délky 7, která jsou řešením homogenní soustavy rovnic s maticí

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha+1 & \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^2+1 \end{pmatrix}.$$

Tj. řešíme pro $c \in \mathbb{F}_2^7$ vektorovou rovnici $Hc^T = 0^T$. Když si soustavu rozepíšeme pro α^0, α^1 a α^2 dostáváme matici:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Nyní vidíme, že náš kód má kontrolní matici $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$, z níž určíme parametry $[7,3,4]_2$. □

Připomeňme, že RS -kód určený prvkem $\alpha \in \mathbb{F}_{q^r}$ řádu n dimenze k je cyklický kód s generujícím polynomem $\prod_{j=0}^{n-k-1}(x-\alpha^j)$ a jím vytvořený r-ární BCH-kód je rovněž cyklický s generujícím polynomem $\mathrm{nsn}\{m_{\alpha^j}, j = 0,\ldots,n-k-1\}$.

4.6. Určete parametry binárního BCH-kódu určeného RS kódem s parametry $[7, 4, 4]_8$.

Opět pracujeme se stejnou prezentací $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ pro $\alpha^3 + \alpha + 1$.

Využijeme popis BCH-kódu jako cyklického kódu, tj., že je jeho generující polynom je právě nsn$\{m_1, m_\alpha, m_{\alpha^2}\}$. Nyní si stačí všimnout, že je α^2 kořenem polynomu x^3+x+1, tedy $m_{\alpha^2} = x^3+x+1 = m_\alpha$, což znamená, že náš BCH-kód je týž jako BCH-kód určený RS kódem s parametry $[7, 5, 3]_8$ z předchozí úlohy, a tudíž má stejné parametry $[7, 3, 4]_2$. □

8.4.

5 Kódování zdroje

5.1 Shannon-Fanovo kódování

5.1. Uvažujme zdroj $X : \Omega \to S = \{0, 1, 2, 3, 4\}$, s pravděpodobnostmi $p_0 = p_1 = \frac{1}{10}$, $p_2 = p_3 = \frac{1}{5}$, $p_4 = \frac{2}{5}$, kde $p_i = P[X = i]$.

(a) Spočítejte binární a ternární entropii zdroje X,

(b) najděte Shannon-Fanovo binární kódování zdroje X a jeho průměrnou délku,

(c) najděte Shannon-Fanovo ternární kódování zdroje X a jeho průměrnou délku,

(a) Přímo spočteme
$H_2 = \frac{2}{10}\log_2(10) + \frac{2}{5}\log_2(5) + \frac{2}{5}\log_2(\frac{5}{2}) = \log_2(5) - \frac{1}{5} \approx 2,12.$
$H_3 = \frac{2}{10}\log_3(10) + \frac{2}{5}\log_3(5) + \frac{2}{5}\log_3(\frac{5}{2}) = \log_3(5) - \frac{1}{5}\log_3(2) \approx 1,34.$

(b) Nejprve určíme délky $l_i := l(C_2(i)) = \left\lceil \log_2 \frac{1}{p_i} \right\rceil$ obrazů jednotlivých slov Shannon-Fanovo binární kódování kódování C_2:

$$l_0 = l_1 = \lceil \log_2 10 \rceil = 4, l_2 = l_3 = \lceil \log_2 5 \rceil = 3, l_4 = \left\lceil \log_2 \frac{5}{2} \right\rceil = 2$$

Nyní snadno určíme průměrnou délku kódování $L_X(C_2) = \frac{2}{10}\cdot 4 + \frac{2}{5}\cdot 3 + \frac{2}{5}\cdot 2 = \frac{14}{5} = 2,8$ i samotné kódování (následující slovo je voleno tak, aby předchozí nebyly jeho prefixem):

$$C_2(4) = 00, \quad C_2(3) = 100, \quad C_2(2) = 010, \quad C_2(1) = 1100, \quad C_2(0) = 1010.$$

(c) Postupujeme obdobně jako v (b). Opět určíme délky $l_i := l(C_3(i)) = \left\lceil \log_3 \frac{1}{p_i} \right\rceil$ obrazů jednotlivých slov Shannon-Fanovo binární kódování kódování C_3:

$$l_0 = l_1 = \lceil \log_3 10 \rceil = 3, l_2 = l_3 = \lceil \log_3 5 \rceil = 2, l_4 = \left\lceil \log_3 \frac{5}{2} \right\rceil = 1,$$

dále spočítáme průměrnou délku kódování $L_X(C_3) = \frac{2}{10} \cdot 3 + \frac{2}{5} \cdot 2 + \frac{2}{5} \cdot 1 = \frac{9}{5} = 1,8$ a možné kódování:

$$C_3(4) = 0, \quad C_3(3) = 10, \quad C_3(2) = 11, \quad C_3(1) = 200, \quad C_3(0) = 201.$$

□

10.4.

5.2. Pro informační zdroj X z předchozího příkladu spočítejte průměrnou délku Shannon-Fanova binárního kódování zdroje X bloky délky 2.

Nejprve spočítáme pravděpodobnosti, délky slov a jejich počty:
Pro pravděpodobnost $\frac{1}{100}$ máme 4 slova délky $\lceil \log_2 100 \rceil = 7$.
Pro pravděpodobnost $\frac{1}{50}$ máme 8 slov délky $\lceil \log_2 50 \rceil = 6$.
Pro pravděpodobnost $\frac{1}{25}$ máme 8 slov délky $\lceil \log_2 25 \rceil = 5$.
Pro pravděpodobnost $\frac{2}{25}$ máme 4 slova délky $\left\lceil \log_2 \frac{25}{2} \right\rceil = 4$.
Pro pravděpodobnost $\frac{4}{25}$ máme 1 slovo délky $\left\lceil \log_2 \frac{25}{4} \right\rceil = 3$.
Nyní spočítáme průměrnou délku kódování zdroje S^2

$$L_2 = \frac{28}{100} + \frac{48}{50} + \frac{40}{25} + \frac{32}{25} + \frac{12}{25} = \frac{115}{25},$$

což znamená, že průměrná délku Shannon-Fanova binárního kódování bloky délky 2 je $\frac{L_{X^2}(C)}{2} = \frac{115}{50} = 2,3$. □

15.4.

5.2 Huffmanovo kódování

5.3. Pro zdroj $S = \{0, 1, 2, 3, 4\}$, s pravděpodobnostmi $p_0 = p_1 = \frac{1}{10}$, $p_2 = p_3 = \frac{1}{5}$, $p_4 = \frac{2}{5}$, kde $p_i = P[\mathcal{S} = i]$ najděte binární Huffmanovo kódování zdroje S a určete jeho průměrnou délku.

	$\forall$	$0 \vee 1 \vee 2 \vee 3$	$2 \vee 3$	$0 \vee 1$	0	1	2	3	4
$S^{(0)}$					$\frac{1}{10}$	$\frac{1}{10}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{2}{5}$
$S^{(1)}$				$\frac{1}{5}$			$\frac{1}{5}$	$\frac{1}{5}$	$\frac{2}{5}$
$S^{(2)}$			$\frac{2}{5}$	$\frac{1}{5}$					$\frac{2}{5}$
$S^{(3)}$		$\frac{3}{5}$							$\frac{2}{5}$
$S^{(4)}$	1								

	$\forall$	$0 \vee 1 \vee 2 \vee 3$	$2 \vee 3$	$0 \vee 1$	0	1	2	3	4
$C^{(0)}$					010	011	000	001	1
$C^{(1)}$				01			000	001	1
$C^{(2)}$			00	01					1
$C^{(3)}$		0							1
$C^{(4)}$	ϵ								

Zkonstruovali jsme Huffmanovo kódování

$$C(4) = 1, \quad C(3) = 001, \quad C(2) = 000, \quad C(1) = 011, \quad C(0) = 010.$$

Vidíme, že průměrnou délka kódování binárního Huffmanova kódu je $L(C) = \frac{2}{5} \cdot 1 + \frac{3}{5} \cdot 3 = \frac{11}{5} = 2,2$. □

5.4. Jsou délky slov Huffmanova kódování určeny až na pořadí jednoznačně?

Budeme-li kódovat tentýž zdroj jako v předchozí úloze, můžeme v redukci $S^{(1)} \to S^{(2)}$ postupovat odlišně:

	$\forall$	$0 \vee 1 \vee 2 \vee 3$	$0 \vee 1 \vee 2$	$0 \vee 1$	0	1	2	3	4
$S^{(0)}$					$\frac{1}{10}$	$\frac{1}{10}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{2}{5}$
$S^{(1)}$				$\frac{1}{5}$			$\frac{1}{5}$	$\frac{1}{5}$	$\frac{2}{5}$
$S^{(2)}$			$\frac{2}{5}$					$\frac{1}{5}$	$\frac{2}{5}$
$S^{(3)}$		$\frac{3}{5}$							$\frac{2}{5}$
$S^{(4)}$	1								

Získáme tak kódování s jinými délkami slov:

	$\forall$	$0 \vee 1 \vee 2 \vee 3$	$0 \vee 1 \vee 2$	$0 \vee 1$	0	1	2	3	4
$\tilde{C}^{(0)}$					0000	0001	000	01	1
$\tilde{C}^{(1)}$				000			001	01	1
$\tilde{C}^{(2)}$			00					01	1
$\tilde{C}^{(3)}$		0							1
$\tilde{C}^{(4)}$	ϵ								

Zkonstruovali jsme tedy Huffmanovo kódování stejného zdroje s jinými délkami než v předchozí úloze

$$\tilde{C}(4) = 1, \quad \tilde{C}(3) = 01, \quad \tilde{C}(2) = 000, \quad \tilde{C}(1) = 0001, \quad \tilde{C}(0) = 0000,$$

průměrná délka kódování ovšem pro optimální kódování musela zůstat stejná (a tedy mezi prefixovými kódováními nejmenší možná): $L(\tilde{C}) = \frac{2}{5} + \frac{2}{5} + \frac{3}{5} + \frac{4}{10} + \frac{4}{10} = \frac{11}{5} = 2,2$. □

5.5. Popište Huffmanovo kódování zdroje velikosti $q = 2^k$ s rovnoměrným rozdělením pravděpodobností a spočítejte jeho průměrnou délku slova.

Všimněme si, že při redukci zdroje $S = S^{(0)}$ s pravděpodobnostmi 2^{-k} má pro každé $i = 0, \ldots, k$ redukovaný zdroj $S^{(2^i-1)}$ rovnoměrné rozdělení s pravděpodobností 2^{i-k}. To znamená, že při konstrukci kódování využijeme všechna slova délky k, tedy Huffmanovým kódováním je libovolná bijekce S na $\mathbb{F}_2^k$ a výsledným kódem je tak úplný binární blokový kód $C(S) = \mathbb{F}_2^k$ délky k. Délka takového kódování je samozřejmě k. □

20.5.

6 Reed-Mullerovy kódy

6.1. Určete parametry a generující matici binárního Reed-Mullerova kódu $\mathcal{R}(3,1)$. Jaký kód dostaneme propíchnutím $\mathcal{R}(3,1)$ v jedné souřadnici?

Protože jsou parametry obecného binárního Reed-Mullerova kódu $\mathcal{R}(m,r)$ právě $[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]_2$, vidíme, že $\mathcal{R}(3,1)$ je $[8,4,4]_2$-kód. To nutně znamená, že propíchnutí má dimenzi 4 a vzdálenost 3 (jinak bychom došli ke sporu s Hammingovým odhadem), snadno nahlédneme, že se jedná právě o kód permutačně ekvivalentní Hammingovu perfektnímu $[7,4,3]_2$-kódu.

Připomeňme, že $\Phi : \mathcal{BP}_3 \to \mathcal{BF}_3$ je zobrazení, které Booleovskému polynomu p přiřadí právě Booleovskou funkci $\mathbf{c} \to p(\mathbf{c})$, kterou reprezentujme slovem $p(\mathbf{c}_0) \ldots p(\mathbf{c}_7)$, kde $\mathbf{c}_i$ je právě trojice cifer z $\mathbb{F}_2$ představující binární zápis čísla i. K nalezení matice stačí spočítat

$$\Phi(1) = 11111111, \Phi(x_1) = 00001111, \Phi(x_2) = 00110011, \Phi(x_3) = 01010101.$$

To znamená, že $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ generující matice kódu $\mathcal{R}(3,1)$. □

6.2. Určete parametry a generující matici binárního Reed-Mullerových kódů $\mathcal{R}(3,0)$ a $\mathcal{R}(3,2)$.

Protože $\Phi(x_\emptyset) = \Phi(1) = 1$, je generující matice $[8,1,8]_2$-kód kódu $\mathcal{R}(3,0)$ tvaru $\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\end{pmatrix}$. Tato matice je zároveň kontrolní maticíc $[8,7,2]_2$-kód $\mathcal{R}(3,2) = \mathcal{R}(3,0)^\perp$. To znamená, že je $\mathcal{R}(3,2)$ paritní kód jehož generující maticí je například $\begin{pmatrix}1&1&0&0&0&0&0&0\\1&0&1&0&0&0&0&0\\1&0&0&1&0&0&0&0\\1&0&0&0&1&0&0&0\\1&0&0&0&0&1&0&0\\1&0&0&0&0&0&1&0\\1&0&0&0&0&0&0&1\end{pmatrix}$. □

Označme $\mathcal{P}_r^m = \{I \subseteq \{1,\dots,m\} \mid |I| \leq r\}$ a $k = |\mathcal{P}_r^m| = \sum_{i=0}^r \binom{m}{i}$. Potom existuje bijekce $b : \{1,\dots,k\} \to \mathcal{P}_r^m$, která indukuje izomorfismsus vektorových prostorů $\beta\mathbb{F}^k \to \mathcal{BP}_m(r)$ předpisem $\beta((a_i)) = \sum_{i=1}^k a_{b(i)} x_{b(i)}$. Jako zdroj kódování můžeme uvažovat $\mathcal{BP}_m(r)$ (místo $\beta\mathbb{F}^k$) a kódování potom určuje dosazovací zobrazení $\Phi : \mathcal{BP}_m(r) \to \mathcal{BF}_m$.

Pro dekódování (po průchodu BSC) přijatého slova (reprezentovaného booleovskou funkcí) na původní booleovský polynom bude sloužit následující algoritmus:

`VSTUP:` $g \in \mathcal{BF}_m$
`VÝSTUP:` $f \in \mathcal{BP}_m(r)$`, pro který` $d(\Phi(f), g) \leq 2^{m-r-1}$
`for d=r downto 0 do`
  `for all` $I \subseteq \{1,\dots,m\} : |I| = d$ `do`
    $\alpha_0 := |\{Y \subseteq \{1,\dots,m\} : Y \cap I = \emptyset, g^I(i_Y) = 0\}|$;
    $\alpha_1 := 2^{m-d} - \alpha_0$ $(= |\{Y \subseteq \{1,\dots,m\} : Y \cap I = \emptyset, g^I(i_Y) = 1\}|)$;
    `if` $\alpha_0 > \alpha_1$ `then` $a_I := 0$ `else` $a_I := 1$, $g := g + \Phi(x_I)$;
`return` $\sum_{I \in \mathcal{P}_r^m} a_I x_I$.

6.3. Pro kódování pomocí RM-kódu $\mathcal{R}(3,1)$ dekódujte přijaté slovo $g = 11000100$ reprezentující boolovskou funkci stejně jako v úloze 6.1.

Budeme používat značení z algoritmu:
Nechť $d = 1$.

$I = \{1\}$: $g^{\{1\}}(i_\emptyset) = \sum_{B:\emptyset\subseteq B\subseteq\{1\}} g(i_B) = g_0 + g_4 = 1 + 0 = 1$,
$g^{\{1\}}(i_{\{2\}}) = \sum_{B:\{2\}\subseteq B\subseteq\{1,2\}} g(i_B) = g_2 + g_6 = 0 + 0 = 0$,
$g^{\{1\}}(i_{\{3\}}) = \sum_{B:\{3\}\subseteq B\subseteq\{1,3\}} g(i_B) = g_1 + g_5 = 1 + 1 = 0$,

$g^{\{1\}}(i_{\{2,3\}}) = \sum_{B:\{2,3\}\subseteq B\subseteq\{1,2,3\}} g(i_B) = g_3 + g_7 = 0 + 0 = 0.$
Tedy $\alpha_0 = 3 > \alpha_1 = 1$ a volíme $a_{\{1\}} := 0$.

$I = \{2\}$: $g^{\{2\}}(i_\emptyset) = \sum_{B:\emptyset\subseteq B\subseteq\{2\}} g(i_B) = g_0 + g_2 = 1 + 0 = 1,$
$g^{\{2\}}(i_{\{1\}}) = \sum_{B:\{1\}\subseteq B\subseteq\{1,2\}} g(i_B) = g_4 + g_6 = 0 + 0 = 0,$
$g^{\{2\}}(i_{\{3\}}) = \sum_{B:\{3\}\subseteq B\subseteq\{2,3\}} g(i_B) = g_1 + g_3 = 1 + 0 = 1,$
$g^{\{2\}}(i_{\{1,3\}}) = \sum_{B:\{1,3\}\subseteq B\subseteq\{1,2,3\}} g(i_B) = g_5 + g_7 = 1 + 0 = 1.$
Tedy $\alpha_0 = 1 < \alpha_1 = 3$ a volíme $a_{\{2\}} := 1$ a
$g := g + \Phi(x_{\{2\}}) = 11000100 + 00110011 = 11110111.$

$I = \{3\}$: $g^{\{3\}}(i_\emptyset) = \sum_{B:\emptyset\subseteq B\subseteq\{3\}} g(i_B) = g_0 + g_1 = 1 + 1 = 0,$
$g^{\{3\}}(i_{\{1\}}) = \sum_{B:\{1\}\subseteq B\subseteq\{1,3\}} g(i_B) = g_4 + g_5 = 1 + 0 = 1,$
$g^{\{3\}}(i_{\{2\}}) = \sum_{B:\{2\}\subseteq B\subseteq\{2,3\}} g(i_B) = g_2 + g_3 = 1 + 1 = 0,$
$g^{\{3\}}(i_{\{1,2\}}) = \sum_{B:\{1,2\}\subseteq B\subseteq\{1,2,3\}} g(i_B) = g_6 + g_7 = 1 + 1 = 0.$
Tedy $\alpha_0 = 3 > \alpha_1 = 1$ a volíme $a_{\{3\}} := 0$.

Nechť $d = 0$.

$I = \emptyset$: Všimněme si, že $g^\emptyset(i_Y) = g(i_Y)$, proto
$g^\emptyset(i_{\{1\}}) = g_4 = 0$ a
$g^\emptyset(i_I) = 1$ pro všechny zbylé množiny $I \neq \{1\}$.
Tudíž $\alpha_0 = 1 < \alpha_1 = 7$ a volíme $a_\emptyset := 1$.

Našli jsme booleovský polynom $x_{\{2\}} + x_\emptyset = x_2 + 1$, pro který snadno ověříme, že $d(g, \Phi(x_2 + 1)) = d(11000100, 11001100) = 1$. □