1 Hammingovy perfektní kódy

1.1 Binární kódy

1.1. Uvažujme polynom $x^3 + x + 1$, který dělí polynom $x^7 - 1$ a označme $\mathcal{C} = \mathcal{C}_2(x^3+x+1)$ binární cyklický $[7, 4]_2$-kód délky 7 generovaný polynomem $x^3 + x + 1 \in \mathbb{Z}_2[x]$.

(a) Najděte generující a kontrolní matici kódu $\mathcal{C}$,

(b) rozhodněte, zda je $v = 1000101$ kódové slovo,

(c) určete vzdálenost kódu $\mathcal{C}$ a rozhodněte, zda je kód perfektní.

(a) Nejprve si uvědomme, že v $\mathbb{Z}_2[x]$ máme ireducibilní rozklad $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

Přímo z definice cyklického kódu 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 $\frac{x^7-1}{x^7-1} = (x + 1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$ 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) Stačí spočítat $(Hv)^T = 010 \neq 000$, což znamená, že $v = 1000101$ kódové slovo není.

(c) Stačí si všimnout, že žádný sloupec kontrolní matice H 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.

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

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) dokažte, 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) ukažte, že je kód $\mathcal{H}_3$ permutačně ekvivalentní kódu z úlohy

(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 H_l je o 1-perfektní kód.

(c) Abychom převedli kód $\mathcal{H}_3$ na $\mathcal{C}_2(x^3 + x + 1)$ stačí, abychom patřičně permutovali sloupce matice H_3 na sloupce matice H. Tj úlohu řeší permutace souřadnic (175364). □

1.3. Označme $\alpha : \mathbb{F}_2^l \setminus \{0\} \to \{1, \ldots, 2^l - 1\}$ 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 $\alpha^{-1}(i)^T$. Ověřte, že pro každé slovo $c \in \mathbb{F}_2^l \setminus \mathcal{H}_l$ platí, že $c + e_{\alpha(cH^T)} \in \mathcal{H}_l$.

Nechť $c \in \mathbb{F}_2^l \setminus \mathcal{H}_l$. Potom je určitě cH^T nenulové slovo, které je rovno právě Stačí si všimnout, že $\alpha(cH_l^T)$ je právě pozice sloupce $H_l c^T$ v matici H_l. To znamená, že $H_l(c + e_{\alpha(cH^T)})^T = H_l c^T + H_l c^T = 0$. □

1.2 q-ární kódy

1.4. 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. □

14.3.

2 GRS a BCH kódy

2.1 Kontrolní matice GRS-kódu

2.1. 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 a určete 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

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

Matice této soustavy má tvar $\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \cdot & \cdot & \ldots & \cdot \\ \alpha_1^{n-k-2} & \alpha_2^{k-1} & \ldots & \alpha_n^{n-k-2} \end{pmatrix}$, 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. □

2.2 Konstrukce GRS a RS kódů

2.2. 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. □

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

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 $[5, 2, 4]_7$ a generující maticí GRS kódu s parametry $[5, 3, 3]_7$.

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 $[5, 3, 3]_7$. □

2.4. Rozhodněte, zda existuje RS-kód s parametry (a) $[5, 3, 3]_q$, (b) $[7, 5, 3]_q$, (c) $[7, 4, 4]_q$.

Existuje-li takový kód, najděte nejmenší q a jeho kontrolní matici.

(a) Hledáme nejmenší 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 nejmenší 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, proto Nyní dopočítáme, že například matice

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

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

2.3 Konstrukce BCH kódů

2.5. 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 $\mathrm{lcm}\{m_{\alpha^j}, j = 0, \ldots, n-k-1\}$.

2.6. 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 $\mathrm{lcm}\{m_0, m_\alpha, m_{\alpha^2}\}$. 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 $[7,3,4]_2$. □

11.4.

3 Kódování zdroje

3.1 Shannon-Fanovo kódování

3.1. Uvažujme 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 $p_i = P[\mathcal{S} = i]$.

(a) Spočítejte binární a ternární entropii zdroje S,

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

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

(d) spočítejte průměrnou délku Shannon-Fanova binárního kódování zdroje S bloky délky 2.

(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 $L(C_2) = \frac{2}{10} \cdot 4 + \frac{2}{5} \cdot 3 + \frac{2}{5} \cdot 2 = \frac{14}{5} = 2,8$ 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 $L(C_3) = \frac{2}{10} \cdot 3 + \frac{2}{5} \cdot 2 + \frac{2}{5} \cdot 1 = \frac{9}{5} = 1,8$ a možné kódování:

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

(d) Nejprve spočítáme pravděpodobnosti, délky slov a jejich počty:
Pro pravdě podobnost $\frac{1}{100}$ máme 4 slova délky $\lceil \log_2 100 \rceil = 7$.
Pro pravdě podobnost $\frac{1}{50}$ máme 8 slov délky $\lceil \log_2 50 \rceil = 6$.
Pro pravdě podobnost $\frac{1}{25}$ máme 8 slov délky $\lceil \log_2 25 \rceil = 5$.
Pro pravdě podobnost $\frac{2}{25}$ máme 4 slova délky $\left\lceil \log_2 \frac{25}{2} \right\rceil = 4$.
Pro pravdě podobnost $\frac{4}{25}$ 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 $L = \frac{L_2}{2} = \frac{115}{50} = 2,3$. □

3.2 Huffmanovo kódování

3.2. 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 $L(C) = \frac{2}{5} \cdot 1 + \frac{3}{5} \cdot 3 = \frac{11}{5} = 2,2$. □

3.3. 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): $L(\tilde{C}) = \frac{2}{5} + \frac{2}{5} + \frac{3}{5} + \frac{4}{10} + \frac{4}{10} = \frac{11}{5} = 2,2$. □

3.4. 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. □

2.5.

4 Designy

4.1 Designy a perfektní kódy

4.1. Nechť $\mathcal{H}_l$ je Hammingův $[2^l-1, 2^l-l-1, 3]_2$-kód z úlohy 1.2 a definujme

$$\mathcal{B} := \{B \subset \{1, \ldots, 2^l - 1\} \mid \ i_B \in \mathcal{H}_l, \ |B| = 3\}.$$

Dokažte, že je $\mathcal{B}$ 2-$(2^l - 1, 3, 1)$-design a 1-$(2^l - 1, 3, 2^{l-1})$-design.

...

□

4.2. Nechť $\mathcal{C}$ je r-perfektní $[n, k, d]_2$-kód a definujme

$$\mathcal{B} := \{B \subset \{1, \ldots, n\} \mid \ i_B \in \mathcal{H}_l, \ |B| = d\}.$$

Dokažte, že je $\mathcal{B}$ $(r + 1)$-$(2^l - 1, 3, 1)$-design.

...

□

4.2 Designy a projektivní roviny

4.3.

□

16.5.

5 Reed-Mullerovy kódy

5.1. 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), což znamená, že se jedná právě é 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 $p(\mathbf{c}_0) \dots p(\mathbf{c}_7)$, 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 $\mathcal{R}(3,1)$. □