# 1 Co jsou lineární kódy

Žádný záznam informace a žádný přenos dat není absolutně odolný vůči chybám. Někdy je riziko poškození zanedbatelné, v mnoha případech je však zaznamenaná a přenášená informace jištěna přidáním dat, která se jeví jako redundantní (nadbytečná) v případě, že nedojde k žádné chybě, která však při výskytu chyby mohou pomoci

- signalizovat, že k chybě došlo,
- případně umožnit její opravu.

Typickým příkladem je přidání paritního bitu. Předpokládejme, že chceme ochránit data složená z hexadecimálních cifer. Každou cifru reprezentujeme čtyřmi bity. Předpokládejme, že data posíláme po kanálu zatíženým značným šumem, a proto přidáme ke každé cifře paritní bit.

Například hexadecimální AF01, což je bitově

$$1010 \mid 1111 \mid 0000 \mid 0001$$

se vyšle jako

$$10100 \mid 11110 \mid 00000 \mid 00011.$$

Takový kód se nazývá paritní a umožní odhalit nejvýše jednu chybu v bloku.

Pokud například při přenosu bloku 10100 dojde při různých přenosech postupně k chybě na pozicích 1, 2, 3, 4 a 5, dostaneme slova 00100, 11100, 10000, 10110, 10101. Pokaždé sice odhalíme, že data byla poškozena, neboť přijatý blok nevyhovuje paritní kontrole – má lichý počet bitů, ale nemáme žádný nástroj, jak určit, na které pozici k chybě došlo. Dvojnásobné chyby neodhalíme vůbec.

Existují lepši zabezpečení? Zdá se, že opravdu bezpečné, i když co do využití místa nepříliš úsporné, by bylo zdvojení každé pozice. Naše zpráva AF01 by pak byla vyslána jako

$$11001100 \mid 11111111 \mid 00000000 \mid 00000011.$$

Nicméně po krátné úvaze uvidíme, že jsme si příliš nepolepšili. Některé dvojnásobné chyby náš kód odhalí, ale pokud k nim dojde na bitech bezprostředně po sobě následujících, tak ji odhalit nemusí. K tomu bychom potřebovali kód, který každou pozici ztrojnásobí. Trojnásobný kód

- signalizuje výskyt dvojnásobných chyb, a
- umožňuje opravit chyby jednonásobné.

Takový kód je ovšem současně značně neúsporný. Čtveřici bitů kóduje dvanácti bity. Ukážeme, že téhož efektu lze dosáhnout kódem, který čtveřici bitů kóduje

pomocí sedmi bitů. Takovému kódu se říká Hammingův a lze jej vytvořit pomocí Fanovy roviny.

Na množině $\{1,\ldots,7\}$ je dáno 7 bloků: $\{1,2,3\}$, $\{3,4,5\}$, $\{1,5,6\}$, $\{1,4,7\}$, $\{2,5,7\}$, $\{3,6,7\}$, $\{2,4,6\}$. Vidíme, že

- Každé dva různé bloky se protínají právě v jednom bodě,
- každými dvěma různými body prochází právě jeden blok,
- existují čtyři body, z nichž žádné tři neleží v jednom bloku.

Systém podmnožin (bloků), který splňuje výše uvedené podmínky, se nazývá projektivní rovina. Blokům se pak obvykle říká přímky. Pokud projektivní rovinu konstruujeme z nějakého systému bodů a přímek, tak pro rozlišení hovoříme o projektivních bodech a projektivních přímkách.

Dříve, než přistoupíme k definici Hammingova kódu, tak poukážeme na roli, kterou v našich úvahách hrají vektorové prostory nad dvouprvkovým tělesem $F = \{0,1\}$.

Zabýváme se **blokovými kódy** určité délky, kterou zpravidla budeme značit $k$. Vstupem jsou tedy prvky $F^k$, což pro nás bude standardní vektorový prostor dimenze $k$. Každý vektor délky $k$ je pak transformován na vektor délky $n$. Při transformaci ovšem nedostaneme všechny vektory délky $n$, ale jenom některé. Každé slovo, které může transformací vzniknout se nazývá **kódové slovo** a jejich sjednocení je **kód**, označíme ho $C$. Je-li $C$ vektorovým podprostorem $F^n$, mluvíme o lineárním $[n,k]$ kódu. Protože za $F$ jsme volili těleso $F_2 = \{0,1\}$, jde o **kód binární**. Stejnou definici je možno použít i pro $F = \mathbb{F}_3$, kdy mluvíme o **kódu ternárním**. Obecně pak **$q$-ární lineární $[n,k]$ kód** je každý podprostor $\mathbb{F}_q^n$, který má dimenzi $k$. Parametr $n$ nazýváme **délka** a parametr $k$ nazýváme **dimenze**.

Pokud v dalším textu bez dalšího vysvětlení zmíníme $[n,k]$ kód, bude se tím rozumět lineární binární kód. Chceme-li stručně naznačit, že jde o lineární $q$-ární kód, píšeme $[n,k]_q$.

Je paritní kód hexadecimálních číslic lineární? Množinu kódových slov můžeme zapsat jako

$$\{(\epsilon_1,\ldots,\epsilon_5);\ \epsilon_1+\ldots+\epsilon_5=0\},$$

a to jistě je vektorový podprostor $\mathbb{F}_2^5$. Jde tedy o binární kód s parametry $[5,4]$.

Každý $[n,k]$ kód $C$ je plně určen $k$-ticí vektorů délky $n$, které udávají jeho generátory. Matice $k\times n$, jejíž řádky generují $C$, se nazývá **generující matice**. Paritní kód délky 5 má generující matici rovnou

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

Tato matice je tvaru $(I\ A)$, kde $I$ je jednotková matice řádu $k$ (zde řádu 4). Takové generující matici se říká **systematická**, nebo také, že je ve **standardním tvaru**.

Ať $G = (I\ A)$ je generující matice nějakého $[n,k]_q$ kódu. Matice $A$ je tedy rozměrů $k \times k'$, kde $k' = n-k$. Ať $g_i = (0,\ldots,0,1,0,\ldots,0,a_{i1},\ldots,a_{ik'})$ je $i$-tý řádek $G$. Je přirozené předpokládat, že vstupní vektor $e_i = (0,\ldots,0,1,0\ldots,0)$, který má 1 v $i$-té pozici, zakódujeme jako $g_i$. Vstupní vektor $u = (\lambda_1,\ldots,\lambda_k)$ zakódujeme tudíž jako $\sum \lambda_i g_i$, což je rovno $u \cdot G$.

Generující matici lze tedy použít pro kódování. Například hexadecimální A se kóduje v paritním kódu jako

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

Kódování lineárních kódů lze tedy realizovat násobením matice a vektoru. Jak realizovat dekódování?

Prvním krokem je určení takzvané **paritní** neboli **kontrolní** neboli **prověrkové** matice $H$. Pro $q$-ární $[n,k]$ kód $C$ je $H$ maticí rozměrů $k' \times n$, kde $k' = n-k$, jež splňuje $u \in C \Leftrightarrow Hu^T = 0$.

Následující tvrzení bude formálně dokázáno až v další kapitole. Jde o standardní fakt, který bývá uváděn i v základních kurzech lineární algebry.

**Tvrzení 1.1.** *Ať $(I\ A)$ je generující maticí ve standardním tvaru. Potom $(-A^T\ I)$ je prověrkovou maticí.*

□

Prověrkovou maticí paritního $[5,4]$ kódu je tedy matice $1 \times 5$ tvaru

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

Jestliže $u$ je vyslané slovo a $w$ je slovo přijaté, tak z $Hw^{\mathsf{T}} \neq 0$ vyplývá, že při přenosu došlo k chybě. Slovo $Hw^{\mathsf{T}}$ se nazývá syndrom a časem ukážeme, jak jej lze využít i pro případnou opravu.

Nyní však potřebujeme vyjasnit, co to přesně znamená, že kód $C$ zachycuje (detekuje) až $r$-násobné chyby a opravuje až $s$-násobné chyby. Pro $u, v \in F^n$, kde $F$ je těleso, položme

$$d(u,v) = |\{i;\ 1 \leq i \leq n, u_i \neq v_i\}|.$$

Pro $u \in F^n$, ať

$$|u| = |\{i;\ 1 \leq i \leq n, u_i \neq 0\}|.$$

Vidíme, že $d(u,v) = |u-v|$. Hodnota $d(u,v)$ se nazývá vzdáleností nebo **Hammingovou vzdáleností** vektorů $u$ a $v$. Hodnota $|u|$ se nazývá **vahou** vektoru $u$.

**Lemma 1.2.** *Ať $u, v, w \in F^n$. Pak $d(u,v) + d(v,w) \geq d(u,w)$.*

*Důkaz.* Ať $R$, $S$ a $T$ jsou po řadě množiny indexů $i$, kde $u_i \neq v_i$, $v_i \neq w_i$ a $u_i \neq w_i$. Jistě $T \subseteq R \cup S$, takže $|T| \leq |R| + |S|$. Přitom $|T| = d(u,w)$, $|R| = d(u,v)$ a $|S| = d(v,w)$. □

Vidíme, že Hammingova vzdálenost vytváří na $F^n$ metriku. Má tedy smysl definovat koule $S(u,r) = \{v \in F^n;\ d(u,v) \leq r\}$, kde $u \in F^n$ je střed a $r$ je poloměr.

Minimální vzdáleností kódu $C$ se rozumí $\min\{d(u,v);\ u,v \in C,\ u \neq v\}$.

**Tvrzení 1.3.** *Ať $C$ je kód s minimální vzdáleností $d$. Pak $C$ detekuje všechny $r$-násobné chyby právě když $r < d$, a $C$ opravuje všechny $r$-násobné chyby právě když $2r < d$.*

*Důkaz.* Ať je vysláno slovo $v$ a přijato slovo $w$. K $r$-násobné chybě dojde právě když $d(v,w) = r$. Jestliže $r$ je menší než $d$, tak nemůže dojít k tomu, aby $w$ bylo považováno za kódové slovo, které by bylo odlišné od $v$. Proto z $r < d$ plyne, že $C$ detekuje všechny $r$-násobné chyby.

Opravit chybu znamená jednoznačně určit nejbližší kódové slovo. Pokud by za nejbližší kódové slovo bylo možné vzít $v' \neq v$, tak máme $r = d(v,w) \geq d(v',w)$ a $2r \geq d(v,w) + d(v',w) \geq d(v,v') \geq d$. Toto nemůže nastat, je-li $2r < d$, takže v takovém případě lze $r$-násobné chyby jednoznačně opravit. Je-li naopak $d \geq 2r$ a $r < d$, tak lze zvolit $v, v' \in C$ a $w$ taková, aby platilo $d = (v,v') = d(v,w) + d(v',w)$. Pak $d - r = d(v',w) \geq d(v,w) \geq r$ a $v$ není možno odvodit z $w$ jako jednoznačně určené nejbližší kódové slovo, což znamená, že chybu nelze jednoznačně opravit. □

Pro nenulový lineární $[n,k]_q$ kód $C$ definujeme jeho minimální váhu jako $\min\{|u|;\ u \in C,\ u \neq 0\}$. Z $d(u,v) = |u - v|$ okamžitě plyne

**Tvrzení 1.4.** *Minimální vzdálenost nenulového lineárního kódu je rovna jeho minimální váze.*

□

Formálně se minimální váha nulového kódu délky $n$ definuje jako $n + 1$. Má-li $[n,k]_q$ kód minimální váhu $d$, hovoříme o $[n,k,d]_q$ kódu. Výše jsme slíbili zkonstruovat binární kód o 16 prvcích, který by opravoval jednonásobné chyby a detekoval až dvojnásobné chyby. Z Tvrzení 1.3 vidíme, že zadání vyhoví každý $[7,4,3]$ kód.

Vraťme se nyní k Fanově rovině. Je-li dán nějaký blok $B \subseteq \{1,\ldots,n\}$, tak jeho incidenční vektor $i_B$ je roven $(\epsilon_1,\ldots,\epsilon_n)$, kde $\epsilon_i = 0$, pokud $i \notin B$ a $\epsilon_i = 1$, pokud $i \in B$.

Ať $w$ je na chvíli binární vektor délky 7, který je tvořen samými jedničkami. Ať $C$ je množina vektorů složená z nulového vektoru, jedničkového vektoru $w$ a vektorů $i_B$ a $w - i_B$, kde $B$ probíhá množinu všech bloků Fanovy roviny. Bloky označme: $B_1 = \{1, 2, 3\}$, $B_2 = \{3, 4, 5\}$, $B_3 = \{1, 5, 6\}$, $B_4 = \{1, 4, 7\}$, $B_5 = \{2, 5, 7\}$, $B_6 = \{3, 6, 7\}$, $B_6 = \{2, 4, 6\}$. Incidenční vektor bloku $B_i$ označme $u_i$. Ať $W$ je podprostor $\mathbb{F}_2^n$ generovaný vektory $u_3$, $u_5$, $u_6$ a $w - u_1$, tedy lineární podprostor generovaný řádky matice

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

**Lemma 1.5.** *Vektorový prostor $W$ se shoduje s množinou $C$.*

*Důkaz.* Množiny $W$ a $C$ mají stejný počet prvků, neboť $\dim W = 4$. Přitom $w \in W$, což lze ověřit součtem všech řádků matice $G$. Zbývá dokázat $\{u_2, u_4, u_7\} \subseteq W$. Ovšem

$$\begin{aligned} u_2 &= (0, 0, 1, 1, 1, 0, 0) = u_6 + (w - u_1), \\ u_4 &= (1, 0, 0, 1, 0, 0, 1) = u_3 + (w - u_1) \text{ a} \\ u_7 &= (0, 1, 0, 1, 0, 1, 0) = u_5 + (w - u_1). \end{aligned}$$

□

S využitím Tvrzení 1.1 můžeme tedy vyslovit

**Tvrzení 1.6.** *Kód $C$ s generující maticí $G$ je binární $[7, 4, 3]$ kód. Jeho prověrková matice je rovna*

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

□

Všimněme si, že ve sloupcích $H$ se vystřídají právě všechny nenulové binární vektory délky 3. Binární Hammingův kód se nazývá každý binární kód, ke kterému lze najít prověrkovou matici s obdobnou vlastností. Jde-li o vektory délky $\ell \geq 2$, dostáváme $[2^\ell - 1, 2^\ell - \ell - 1, 3]$ kód, což v obecnosti dokážeme až v další kapitole. Výše zkonstruovaný kód $C$ odpovídá případu $\ell = 3$; budeme hovořit o základním Hammingově kódu.

Při definici Hammingova kódu neurčujeme pořadí sloupců, jde jen o to, aby se vystřídaly všechny vektory. Obecně se kódy často definují až na pořadí souřadnic. Říká se, že kódy $C_1$ a $C_2$ délky $n$ jsou permutačně ekvivalentní, jestliže existuje $\sigma \in S_n$, že $(u_1, \ldots, u_n) \in C_1 \Leftrightarrow (u_{\sigma(1)}, \ldots, u_{\sigma(n)}) \in C_2$.

# 2 Hrátky s maticemi

Obecně lze blokový kód délky $n$ definovat jako neprázdnou podmnožinu $C$ množiny $\mathbb{A}^n$, kde $\mathbb{A}$ je nějaká neprázdná konečná množina. $\mathbb{A}$ je zvykem nazývat **abecedou**. Je-li $|\mathbb{A}| = q$, hovoříme o $q$-árním kódu. Kód je lineární, jestliže $\mathbb{A}$ lze ztotožnit s $\mathbb{F}_q$ tak, aby $C$ bylo lineárním podprostorem. Pokud $q$ není mocnina prvočísla, tak samozřejmě o lineární kód jít nemůže.

Má-li $C \subseteq \mathbb{A}^n$ právě $h$ prvků, hovoříme o $(n, h)$ kódu, případně o $(n, h)_q$ kódu. Lineární kód délky $n$ a dimenze $k$ je tedy $[n, k]_q$ kódem a $(n, q^k)_q$ kódem.

**Minimální vzdálenost** kódu $C$ je rovna $\min\{d(u, v)\}$, kde $u, v \in C$ a $u \neq v$. Má-li kód $C$ jediný prvek, je jeho minimální vzdálenost rovna $n + 1$. Známe-li minimální vzdálenost $d$, značíme $(n, h)_q$ kód jako $(n, h, d)_q$ kód. Pro obecně nelineární kódy platí tvrzení 1.3 v nezměněné podobě, na důkazu není třeba nic měnit.

Většinou, avšak ne výhradně, se budeme zabývat kódy lineárními. Nelineární blokové kódy budeme uvažovat zejména tehdy, když budeme chtít vyložit, že určitý lineární kód poskytuje optimální chování, které nelze vylepšit ani při přechodu ke kódu nelineárnímu.

Pro $(n, h)_q$ kód $C$ definujeme **informační poměr** (anglicky rate, jako český jednoslovný ekvivalent budeme používat též slovo **nosnost**) jako zlomek $\frac{\log_q h}{n}$. Pro $[n, k]_q$ kód je nosnost rovna $k/n$. Informační poměr udává, jaká část zakódované zprávy je potřebná ke sdělení jejího informačního (nekódovaného) obsahu. Cílem teorie kódů je navrhnout kódy, které při zadaném informačním poměru opravují efektivně co nejvíce chyb; případně při zadané schopnosti opravovat maximalizují informační poměr. V praxi se ukazuje jako nutné reagovat na skutečnost, že chyby nebývají rozděleny náhodně, ale vyskytují se ve shlucích. Základem teorie samoopravných kódů jsou však lineární kódy konstruované s předpokladem náhodného výskytu chyby.

Buď $F$ komutativní těleso. Při práci s lineárními kódy má zásadní význam **bodový součin** $u \cdot v = \sum_{i=1}^{n} u_i v_i$ pro vektory $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in F^n$. V případě $F = \mathbb{R}$ jde o součin skalární. Někdy se bodový součin nazývá skalární i nad jinými tělesy, není to však přesné. Je-li například $F = \{0, 1\}$, tak $u \cdot u = 0$ právě když $|u| \equiv 0 \bmod 2$.

Z terminologie skalárního součinu si nicméně vypůjčíme pojem **ortogonální doplněk**. Je-li $M \subseteq F^n$, tak ortogonální doplněk $M^\perp = \{v \in F^n;\ v \cdot u = 0\ \forall u \in M\}$. Lineární obal množiny $M$ budeme značit $\langle M \rangle$.

**Lemma 2.1.** *Pro každé $u$, $v$, $w \in F^n$ je*

- $u \cdot v = v \cdot u$
- $u \cdot (v + w) = u \cdot v + u \cdot w$
- $\forall \lambda \in F$ *je* $u \cdot (\lambda v) = \lambda (u \cdot v)$

*Tedy $\cdot$ je symetrická bilineární forma na $F^n$.*

□

**Lemma 2.2.** *Buď $M$, $N \subseteq F^n$. Pak*

- *$M^\perp$ je lineární podprostor $F^n$*
- *$\langle M \rangle^\perp = M^\perp$*
- *$M \subseteq \left(M^\perp\right)^\perp$*
- *z $M \subseteq N$ plyne $M^\perp \supseteq N^\perp$*

□

**Lemma 2.3.** *Pro $M$, $N \subseteq F^n$ je $(M \cup N)^\perp = M^\perp \cap N^\perp$. Pokud $0 \in M \cap N$, tak $(M \cup N)^\perp = (M + N)^\perp$, kde $M + N = \{u + v;\, u \in M,\, v \in N\}$.*

□

Důkazy těchto tvrzení není třeba uvádět. Jsou snadné a odpovídají důkazům známým pro skalární součin.

Je-li $u = (\lambda_1, \ldots, \lambda_n) \in F^n$, $u \neq 0$, tak $u^\perp = \{(a_1, \ldots, a_n) \in F^n;\, \sum_{i=1}^n \lambda_i a_i = 0\}$ je zjevně podprostor dimenze $n-1$. Takovým podprostorům se říká **nadrovina**. Je-li $U \subseteq F^n$ podprostor dimenze $k$ a $W$ je nadrovina, tak buď $U \subseteq W$, nebo $U \cap W$ má dimenzi $k-1$.

Buď nyní $0 = U_1 \subset U_1 \subset \ldots \subset U_n = F^n$ řada do sebe vložených podprostorů. Vidíme, že $\dim U_j = j$. Zvolme bázi $e_1, \ldots, e_n$ prostoru $F_n$ tak, aby $U_{i+1} = \langle U_i, e_{i+1} \rangle$, $0 \leq i \leq n-1$. Podle Lemmatu 2.3 je $U_j^\perp = U_{j-1}^\perp \cap e_j^\perp$. Proto má $U_j^\perp$ dimenzi nejvýše o jedničku menší, než $U_{j-1}^\perp$. Máme

$$0 = U_n^\perp \subseteq U_{n-1}^\perp \subseteq \cdots \subseteq U_1^\perp \subseteq U_0^\perp = F^n,$$

přičemž sousední podprostory se liší v dimenzi nanejvýš o jedničku. Jestliže jich je $n+1$, musí být $\dim U_j^\perp = n - j$.

Je-li dán podprostor $V \subseteq F^n$ dimenze $k$, tak lze jistě sestrojit $0 = U_1 \subset U_1 \subset \ldots \subset U_n = F^n$ tak, aby $V$ bylo rovno některému $U_j$, $0 \leq j \leq n$. Proto platí

**Lemma 2.4.** *Ať $V$ je podprostor $F^n$. Pak $\dim V + \dim V^\perp = n$ a $\left(V^\perp\right)^\perp = V$.*

□

Ať $C$ je $[n,k]_q$ kód. Z lemmatu 2.4 plyne, že $C^\perp$ je $[n, n-k]_q$ kód. Ať $H$ je generující matice $C^\perp$. Označme její řádky $v_1, \ldots, v_{k'}$, kde $k' = n-k$. Víme, že $C^\perp = \langle v_1, \ldots, v_{k'} \rangle$, takže $\left\{u \in F^n; Hu^T = 0\right\} = \{v_1, \ldots, v_{k'}\}^\perp = \left(C^\perp\right)^\perp = C$. Dokázali jsme:

**Tvrzení 2.5.** *Generující matice doplňkového kódu $C^\perp$ se shodují s prověrkovými maticemi kódu $C$.*

□

Ze znalosti generující matice není často snadné zjistit minimální váhu kódu. Někdy může pomoci následující pozorování:

**Tvrzení 2.6.** *Ať $C$ je $[n,k,d]_q$ kód s prověrkovou maticí $H$. Potom platí, že $d-1$ je rovno největšímu číslu $r$ takovému, že každých $r$ sloupců $H$ je lineárně nezávislých.*

*Důkaz.* Případ $r=0$ nastává právě tehdy, je-li alespoň jeden ze sloupců matice $H$ nulový. V takovém případě je zjevně $d=1$. Ať $r \geq 1$ a ať kódové slovo $(\lambda_1,\ldots,\lambda_n) \in C$ má právě $t>0$ nenulových hodnot $\lambda_i$. Zvolíme-li řádek $H$, jenž je nenulový v některém sloupci $i$, pro který platí $\lambda_i \neq 0$, tak vidíme, že odpovídajících $t$ sloupců je lineárně závislých. Proto $t \geq r+1$. Je-li $C=0$, tak $d=n+1$ a $r=n$. Předpokládejme, že $C \neq 0$. Pak lze volit $t=d$, takže $d-1 \geq r$. Současně víme, že existuje vektor $u=(\lambda_1,\ldots,\lambda_n)$ s právě $r+1$ nenulovými hodnotami takový, že $Hu^\mathsf{T}=0$. To znamená, že $u \in C$, a proto $r+1 \geq d$. □

**Důsledek 2.7.** *Ať $C$ je $[n,k,d]_q$ kód. Potom $d \leq n-k+1$.*

*Důkaz.* Provérková matice $H$ může obsahovat regulární matici řádu $s$ nanejvýše pro $s=n-k$ (to je počet řádků). Proto $d-1 \leq n-k$. □

Výše uvedená nerovnost se nazývá **Singletonův odhad**. Platí i pro nelineární kódy. Lineární kódy, ve kterých $d=n-k+1$, se nazývají **MDS** (maximum distance separable). Z Důsledku 2.7 okamžitě plyne jejich charakterizace pomocí prověrkové matice:

**Důsledek 2.8.** *Ať $C$ je $[n,k,d]_q$ kód s prověrkovou maticí $H$. Kód $C$ je MDS právě když každá její čtvercová podmatice řádu $n-k$ je regulární.*

Zvolme $\ell \geq 2$ a ať $F=\mathbb{F}_q$, $V=F^\ell$ a $V^\# = V\backslash\{0\}$. Na $V^\#$ definujeme ekvivalenci $\sim$ tak, že $u \sim v$ právě když $u=\lambda v$ pro nějaké $\lambda \in F^*$. Vidíme, že $u \sim v$ právě když $\langle u\rangle = \langle v\rangle$. Každý blok $\sim$ má $q-1$ prvků, takže máme $n=\frac{q^\ell-1}{q-1}$ bloků. Z každého z nich vybereme jeden prvek a vybrané prvky označíme $v_1,\ldots,v_n$. Pro $1 \leq i < j \leq n$ platí $\langle v_i\rangle \neq \langle v_j\rangle$ takže $v_i$ a $v_j$ jsou lineárně nezávislé. Ovšem pro $\ell \geq 3$ zjevně existují lineárně závislé vektory $v_i$, $v_j$ a $v_k$, kde $1 \leq i < j < k \leq n$. Sestavme prověrkovou matici $H$ tak, aby sloupce byly tvořeny vektory $v_1,\ldots,v_k$. Z Tvrzení 2.6 plyne, že $H$ určuje $[n,\ell,3]$ kód. Všechny takové kódy se nazývají **Hammingovy**. Vidíme také, že v případě binárních kódů je matice $H$ určena až na pořadí sloupců jednoznačně, neboť každý blok $\sim$ obsahuje jediný prvek.

Hammingovy kódy se snadno dekódují. Zabývejme se znovu na chvíli otázkou dekódování $[n,k,d]_q$ kódu $C$ pomocí jeho prověrkové matice $H$. Ať $v$ je vyslané

kódové slovo, a ať $w$ je slovo přijaté. Rozdílu $e = w - v$ se říka slovo **chybové**. Vidíme, že $Hw^T = He^T$. Jinak řečeno, slovo chybové i přijaté mají stejný syndrom. Je-li $Hw^T \neq 0$, tak pro připadnou opravu hledáme kódové slovo $v$, aby $|w - v|$ bylo co nejmenší. To znamená, že hledáme $e$ takové, aby $|e|$ bylo co nejmenší a $w - e \in C$. Ovšem $w - e \in C$ právě když $Hw^T = He^T$.

**Opravit přijaté slovo na nejbližší kódové slovo tedy znamená pro daný syndrom nalézt slovo nejmenší váhy s týmž syndromem. Je-li takové slovo jediné, je oprava jednoznačná.**

Došlo-li k chybě v jediné pozici, řekněme $j$, tak je syndrom roven $j$-tému sloupci matice $H$. Pokud pro binární Hammingův kód vytvoříme $H$ pomocí lexikografického uspořádání tak, že $j$-tý sloupec je roven $(i_0, \ldots, i_{l-1})$ právě když $j = \sum i_r 2^r$, tak ze syndromu $(e_0, \ldots, e_{l-1}) \neq 0$ dostaneme chybovou pozici okamžitě jako $\sum e_r 2^r$.

Obecně je počet syndormů roven $q^{n-k}$. Pokud je tato hodnota dostatečně malá, aby ji bylo možno použít jako index tabulky, tak lze ke každému syndromu $s$ nalézt $e_s$ takové, že $s = He_s^\mathsf{T}$ a $|e_s|$ je minimální možná. Algoritmus dokódování se pak redukuje na určení syndromu $s = Hw^\mathsf{T}$, opravu $v = w - e_s$ a nalezení $u$, že $v = Gu^\mathsf{T}$. Poslední krok je ovšem triviální, je-li generující matice $G$ ve standardním tvaru. Pak je $u$ shodné s prvými $k$ symboly $v$.

***

Kód $C$ se nazývá **samoortogonální**, jestliže $C \subseteq C^\perp$. Je-li $C = C^\perp$, hovoříme o kódu **samoduálním**. Zvláště důležité jsou binární samoduální kódy s vysokou minimální vahou. Z lemmatu 2.2 vidíme, že lineární kód s generující maticí $G$ je samoortogonální, právě když $u \cdot v = 0$ platí pro libovolné dva řádky $u$, $v$ matice $G$.

Pro samoduální $[n, k, d]_q$ kód $C$ musí platit $n = \dim C + \dim C^\perp = 2 \dim C$. Samoduální kódy mohou existovat tedy pouze pro sudou délku. Lze říci, že to jsou samoortogonální kódy maximální možné dimenze (pro samoortogonální kód máme $n = \dim C + \dim C^\perp \geq 2 \dim C$).

Při práci s binárními vektory je zvykem pro $u, v \in \mathbb{F}_2^n$ označit $u \cap v$ ten vektor $w \in \mathbb{F}_2^n$, pro který $w_j = 1$ právě když současně $u_j = 1$ a $v_j = 1$. Je-li tedy $u = i_A$, $v = i_B$, tak $u \cap v = i_{A \cap B}$.

Zásadního významu pro práci s binárními kódy je toto jednoduché pozorování:

**Lemma 2.9.** *Ať $u$ a $v$ jsou binární vektory délky $n$. Pak $|u + v| = |u| + |v| - 2|u \cap v|$ a $|u \cap v| \equiv u \cdot v \pmod 2$.*

*Důkaz.* Pro $A, B \subseteq \{1, \ldots, n\}$ označme na chvíli $A \triangle B$ disjunktní sjednocení $(A \cup B) \setminus (A \cap B)$. Ať $u = i_A$ a $v = i_B$. Máme $u + v = i_{A \triangle B}$, takže dokazovaná rovnost je totéž jako $|A \triangle B| = |A| + |B| - 2|A \cap B|$, což zřejmě platí. Vidíme také, že $u \cdot v$ je součtem tolika jedniček, kolik jich je v $u \cap v$. Proto platí i druhý vztah (Jeho zápisu lze po formální stráce vytknout, že porovnává $u \cdot v$, což je prvek $\mathbb{F}_2$, s celým číslem $|u \cap v|$. Jde však o zápis běžně používaný.) □

Binární kód se $C$ se nazývá **dvojnásobně sudý**, jestliže váha každého kódového slova $u \in C$ je dělitelná čtyřmi.

**Lemma 2.10.** *Ať $C$ je samoortogonální binární lineární kód s generující maticí $G$. Ať $u_1, \ldots, u_k$ jsou řádky $G$. Jestliže je váha každého řádku $G$ dělitelná čtyřmi, tak je kód $C$ dvojnásobně sudý.*

*Důkaz.* Prvky $C$ jsou právě všechny součty řádků z $G$. Proto stačí ukázat, že pro libovolná $u$, $v \in C$ taková, že $|u|$ a $|v|$ jsou dělitelná čtyřmi, platí, že čtyři dělí i $|u+v|$. Z lemmatu 2.9 plyne, že $2|u \cap v| \equiv 0 \bmod 4$ pro všechna $u$, $v \in C$, neboť $C$ je samoortogonální, a tedy $|u \cap v| \equiv 0 \bmod 2$. Tudíž $|u+v| \equiv |u|+|v| \bmod 4$. □

Ať $C$ je $[n,k,d]_q$ kód s generující maticí $G$. Kód $C$ je samoortogonální právě když platí $\langle u_1, \ldots, u_k \rangle \subseteq \langle u_1, \ldots, u_k \rangle^\perp = \{u_1, \ldots, u_k\}^\perp$, a to nastává právě když $\{u_1, \ldots, u_k\} \subseteq \{u_1, \ldots, u_k\}^\perp$ (viz Lemma 2.2). Můžeme tedy vyslovit následující lemma, které se často používá společně s Lemmatem 2.10.

**Lemma 2.11.** *Ať $C$ je $[n,k,d]_q$ kód s generující maticí $G$. Kód $C$ je samoortogonální právě když $u \cdot v = 0$ platí pro libovolné dva řádky matice $G$.*

□

Na závěr této kapitoly uvedeme několik pozorování, která se týkají nelineárních kódů.

**Lemma 2.12.** *Ať $C$ je binární $(2k, 2^k)$ kód. Jestliže $u \cdot v = 0$ pro všechna $u$, $v \in C$, tak $C$ je lineárním samoduálním kódem.*

*Důkaz.* Z $C \subseteq C^\perp$ plyne $\langle C \rangle \subseteq C^\perp$ a $\langle C \rangle \subseteq \langle C \rangle^\perp$. Ať $h = \dim C$. Máme $h \leq 2k - h$, a tedy $h \leq k$. Lineární prostor $\langle C \rangle$ tedy obsahuje nejvýše $2^k$ prvků. Proto musí platit, že $C = \langle C \rangle$. □

**Lemma 2.13.** *Ať $C$ je binární kód, který obsahuje 0. Předpokládejme, že pro každé $u \in C$ je $u + C$ dvojnásobně sudý lineární kód. Potom $u \cdot v = 0$ pro všechna $u$, $v \in C$.*

*Důkaz.* Pro $u, v \in C$ máme $u+v \in u+C$, takže vektory $u$, $v$ i $u+v$ mají váhu dělitelnou čtyřmi. Lemma proto plyne z Lemmatu 2.9. □

**Důsledek 2.14.** *Ať $C$ je binární $(2k, 2^k)$ kód takový, že $0 \in C$, a že $u + C$ je dvojnásobně sudý kód pro každé $u \in C$. Potom $C$ je lineární samoduální kód.*

□

# 3 Designy a konstrukce lineárního Golayova kódu

Fanovu rovinu lze chápat jako systém trojbodových podmnožin, který má tu vlastnost, že každá dvojbodová pomnožina leží právě v jedné trojbodové množině tohoto systému. Každý takový systém se nazývá **Steinerův systém trojic**. (Steiner triple system, STS). Fanova rovina je STS na sedmi bodech. Není obtížné dokázat, že STS na $v$ bodech existuje právě když $v \equiv 1 \bmod 6$ nebo $v \equiv 3 \bmod 6$. STS na 9 bodech snadno zkonstruujeme z matice $3\times3$, kde 6 trojic je tvořeno řádky a sloupci a dalších 6 trojic získáme jako $\{(i, \sigma(i)); 1 \leq i \leq 3\}$, kde $\sigma$ probíhá $S_3$. Tyto trojice tvoří známé schéma počítání determinantu matice řádu 3.

Počet trojic v STS velikosti $v$ lze snadno odvodit. Máme $\binom{v}{2}$ dvojic a každá z nich určuje jednoznačně některou z $b$ trojic. Každá trojice je určena právě třemi dvojicemi, takže musí platit $\binom{v}{2} = 3b$.

Zvolíme-li pevně nějaký bod $A$ nosné množiny, tak ten leží ve $v-1$ dvojicích. Označíme-li $r$ počet trojic, které obsahují daný bod, tak dostaneme $2r = v-1$, neboť každá z $r$ trojic je určena dvěma různými body odlišnými od bodu $A$.

Podmínka $v \equiv 1, 3 \bmod 6$ je vyjádřením podmínky, aby $v-1$ bylo dělitelné 2 a $\binom{v}{2}$ bylo dělitelné třemi. Dokázali jsme, že každý STS musí tuto podmínku splňovat.

Obecnější pojem než STS jsou designy. Řekneme, že systém bloků $\mathcal{B}$ na množině $X$ je $t{-}(v, k, \lambda)$ **design**, jestliže

- $|X| = v$
- $k = |B|$ pro každé $B \in \mathcal{B}$
- každá $t$-bodová podmnožina $X$ je obsazena v právě $\lambda$ blocích $\mathcal{B}$.

STS na $v$ bodech je $2{-}(v, 3, 1)$ design. V teorii designů se připouští, aby se některé bloky $\mathcal{B}$ mohly opakovat (čili taková podmnožina může figurovat v $\mathcal{B}$ vícekrát). Designům bez opakování se říká **jednoduché**. Zde se budeme zabývat pouze jednoduchými designy a v dalším se tedy pod slovem design myslí jednoduchý design. Zaměříme se zejména na $2-(v, k, \lambda)$ designy.

Následující tvrzení zobecňuje úvahy, které jsme již učinili v případě Steinerova systému trojic.

**Tvrzení 3.1.** *Ať $\mathcal{B}$ je $2{-}(v, k, \lambda)$ design. Označme $b$ počet bloků. Potom*

$$\lambda v(v-1) = bk(k-1).$$

*Pro $k \geq 2$ navíc platí, že existuje číslo $r$, které pro každý bod nosné množiny určuje počet bloků, jež tento bod obsahuje, a které splňuje $\lambda(v-1) = r(k-1)$.*

*Důkaz.* Počítejme velikost $w$ množiny

$$W = \{(A, B);\ B \in \mathcal{B}, A \subseteq B \text{ a } |A| = 2\}.$$

Máme $\binom{v}{2}$ možností pro $A$, takže $w = \lambda\binom{v}{2}$. Současně pro daný blok $B$ můžeme zvolit $\binom{k}{2}$ dvojic $A$ obsažených v $B$, odkud $w = b\binom{k}{2}$.

Druhou rovnost pak obdržíme podobnou úvahou, když místo $W$ uvažujme její podmnožinu složenou ze všech $(A, B)$, kde $A$ obsahuje daný vybraný bod. □

Význam písmen $v$, $k$, $\lambda$, $b$ a $r$ se v dalším výkladu o designech nebude měnit.

**Důsledek 3.2.** *V každém* $2{-}(v, k, \lambda)$ *designu, kde* $k \geq 2$*, platí* $rv = bk$*.*

□

Ať $\mathcal{B}$ je $t{-}(v, k, \lambda)$ design a ať $B_1, \ldots, B_b$ a $x_1, \ldots, x_v$ jsou nějaká lineární uspořádání bloků $\mathcal{B}$ a bodové nosné množiny. V našich úvahách bude značnou roli hrát *incidenční matice* $M$, jejíž $j$-tý řádek je roven incidenčnímu vektoru $i_{B_j}$.

Následující lemma má charakter pozorování, a proto je uvedeno bez důkazu.

**Lemma 3.3.** *Ať* $M$ *je incidenční matice* $2{-}(v, k, \lambda)$ *designu. Položme* $U = MM^T$ *a* $V = M^TM$*. Potom*

- $U = (u_{ij})$ *a* $V = (v_{ij})$ *jsou symetrické čvtercové matice řádů* $b$ *a* $v$*.*
- $u_{ii} = k$ *pro každé* $i \in \{1, \ldots, b\}$
- $v_{jj} = r$ *pro každé* $j \in \{1, \ldots, v\}$
- *Je-li* $1 \leq i < j \leq b$*, tak* $u_{ij} = |B_i \cap B_j|$
- *Je-li* $1 \leq i < j \leq v$*, tak* $v_{ij} = \lambda$*.*

□

Matici $V = M^TM$ můžeme zapsat jako $(r - \lambda)I + \lambda J$, kde $I$ je jednotková matice a $J$ je matice jedničková (tedy matice, která má hodnotu 1 v každé pozici). Z kontextu je zřejmé, že $I$ i $J$ jsou čtvercové matice řádu $v$. Pro další úvahy bude důležité, že matice $V$ je invertibilní:

**Lemma 3.4.** *Pro každé* $n \geq 1$ *platí, že* $\det(sI + tJ) = (s + nt)s^{n-1}$*.*

*Důkaz.* Odečteme nejprve poslední sloupec matice ode všech předchozích a pak přičteme součet všech předchozích řádků k poslednímu. Získáme matici, která má na hlavní diagonále hodnotu $s$ ve všech řádcích mimo posledního, v dolním pravém rohu má hodnotu $s + nt$, a všude pod diagonálou má nuly. □

**Věta 3.5.** *Ať* $k \geq 2$*. Ať* $\mathcal{B}$ *je systém* $k$*-bodových podmnožin* $v$*-bodové množiny* $X$ *a ať* $v = |\mathcal{B}|$*. Předpokládejme, že každý bod množiny* $X$ *leží ve stejném počtu bloků. Potom je tento počet roven* $k$ *a platí, že* $\mathcal{B}$ *je* $2 - (v, k, \lambda)$ *design právě když pro každé dva různé bloky* $B$ *a* $C$ *je* $|B \cap C| = \lambda$*.*

*Důkaz.* Označme $M$ incidenční matici designu $\mathcal{B}$ a použijme stejné označení jako v Lemmatu 3.3. Matice $U$ a $V$ jsou čtvercové řádu $v$. Protože předem nepředpokládáme, že $\mathcal{B}$ je nutně 2-design, tak o $V$ pouze víme, že je symetrickou maticí, kde $v_{ij}$ udává počet bloků, které obsahují prvky $x_i$ a $x_j$.

Součet hodnot na diagonále je jak pro $U$ tak pro $V$ roven velikosti množiny $\{(x, B);\ x \in B \text{ a } B \in \mathcal{B}\}$. Podle předpokladů věty jsou hodnoty $u_{ii}$ (velikost $i$-tého bloku) a $v_{ii}$ (počet bloků obsahujících bod $x_i$) na volbě $i$ nezávislé. Proto $k = v_{ii} = u_{ii}$ pro každé $i$, $1 \leq i \leq k$.

Tvrzení věty lze tedy vyjádřit vztahem

$$MM^{\mathsf{T}} = (k-\lambda)I + \lambda J \ \Leftrightarrow\ M^{\mathsf{T}}M = (k-\lambda)I + \lambda J.$$

Determinant matice $(k-\lambda)I+\lambda J$ je podle Lemmatu 3.4 roven $(k-\lambda)^{n-1}(k+(v-1)\lambda)$. Případ $k = \lambda$ lze opominout, neboť ten, jak lze nahlédnout například s použitím Tvrzení 3.1, v obou případech znamená, že $\mathcal{B}$ obsahuje jediný blok, odkud $v = 1 = k$. Ať tedy je $k > \lambda$. Potom $\det M \neq 0$, neboť $\det MM^{\mathsf{T}} = \det M^{\mathsf{T}}M = (\det M)^2$. Vztah $MM^{\mathsf{T}} = M^{\mathsf{T}}M$ lze pak vyjádřit jedank jako $M^{-1}(MM^{\mathsf{T}})M = MM^{\mathsf{T}}$, jednak jako $M(M^{\mathsf{T}}M)M^{-1} = M^{\mathsf{T}}M$. Protože předpokládáme, že známe vyjádření $MM^{\mathsf{T}}$ nebo vyjádření $M^{\mathsf{T}}M$, tak pro dokončení důkazu stačí ověřit, že $M$ komutuje s maticí $(k-\lambda)I+\lambda J$. Protože $M$ jistě komutuje s $I$, jde o to, zda komutuje s $J$. Matice $MJ$ má v každé buňce hodnotu $k$, neboť všechny bloky $\mathcal{B}$ jsou velikosti $k$. Matice $JM$ má ovšem v každé buňce také hodnotu $k$, neboť každý bod leží přesně v $k$ blocích. □

Systémy, které vyhovují větě 3.5, se nazývají **čtvercové (kvadratické) designy**, někdy též **symetrické designy**. Jsou to 2–$(v, k, \lambda)$ designy, které mají právě $v$ bloků. Rovnosti z Tvrzení 3.1 se redukují na $r = k$ a $\lambda(v-1) = k(k-1)$. V těchto desginech je role bodu a bloku záměnná, neboť transponováním incidenční matice vznikne matice, která je rovněž incidenční maticí 2-designu.

Pro další výklad jsou důležité 2$-(11, 5, 2)$ designy. Z rovnosti $\lambda v(v-1) = bk(k-1)$ uvedené v Tvrzení 3.1 plyne, že $220 = 20b$, tedy $b = v = 11$. Takže tyto designy jsou čvercové.

Položme $Y = \{1, 2, 3, 4, 5\}$ a ať $X$ je množina všech dvouprvkových podmnožin $Y$. Grafem na $Y$ rozumíme nějakou podmnožinu $X$. Je-li dán graf na $Y$ takový, že z každého vrcholu vycházejí právě dvě hrany, vidíme, že takový graf propojuje všechny vrcholy $Y$. Tedy tvoří pěticyklus. Každý pěticyklus lze orientovat dvěma způsoby, a každá z těchto orientací poskytuje permutaci $\varphi \in S_5$ řádu 5. Opačná orientace samozřejmě dává inverzní permutaci $\varphi^{-1}$. Položme $P = \{\varphi \in S_5, |\varphi| = 5\}$. Pro každé $\varphi \in P$ ať $P_\varphi = \{\{i, \varphi(i)\}, i \in Y\}$. Vidíme, že $P_\varphi$ je pěticyklus a že každý pěticyklus lze vyjádřit tímto způsobem. Pro $\varphi$, $\psi \in P$ máme $P_\varphi = P_\psi$ právě když $\varphi = \psi^{\pm 1}$. Na $Y$ tedy existuje $12 = |P|/2$ pěticyklů.

Pro $\varphi$, $\psi \in P$ ať $t(\varphi, \psi) = |\{i \in Y;\ \psi(i) = \varphi^{\pm 1}(i)\}|$. Zjevně $t(\varphi, \psi) = |P_\varphi \cap P_\psi|$. Jelikož $P_{\varphi^2} \cup P_\varphi = X$, tak $t(\varphi, \psi) + t(\varphi^2, \psi) = 5$. Dva pěticykly na $Y$, které

se shodují ve čtyřech hranách se již shodují zcela, takže $t(\varphi,\psi) \notin \{1,4\}$. Zřejmě $t(\varphi,\psi) = 5 \Leftrightarrow \psi = \varphi^{\pm 1}$ a $t(\varphi,\psi) = 0 \Leftrightarrow \psi = \varphi^{\pm 2}$. Pro zbylých 20 permutací $\psi$ platí buď $t(\varphi,\psi) = 2$ a $t(\varphi^2,\psi) = 3$, nebo $t(\varphi,\psi) = 3$ a $t(\varphi^2,\psi) = 2$. Obě skupiny jsou zjevně stejně velké.

**Lemma 3.6.** *Definujme na $P$ relaci $\rho$ tak, že $(\varphi,\psi) \in \rho \Leftrightarrow t(\varphi,\psi) \in \{0,2\}$. Tato relace je ekvivalence a každá její ekvivalenční třída má 12 prvků.*

*Důkaz.* Potřebujeme dokázat, že $\rho$ je tranzitivní relace. Ať $(\varphi,\psi) \in \rho$ a $(\varphi,\psi') \in \rho$. Případy $\psi = \varphi^{\pm 1}$, $\psi' = \varphi^{\pm 1}$ a $\psi' = \psi^{\pm 1}$ jsou triviální, takže předpokládáme, že žádný z nich nenastává. Cílem je tedy ukázat, že

$$t(\varphi,\psi) = t(\varphi,\psi') = 2 \text{ a } \psi' \neq \psi^{\pm 1} \Rightarrow t(\psi,\psi') = 2.$$

Prvky $Y$ můžeme případně přejmenovat, tak aby cyklický zápis permutace $\varphi$ byl roven (1 2 3 4 5). Definujme $\varphi_i$ jako permutaci ($i{+}1$ $i{+}2$ $i$ $i{-}2$ $i{-}1$). Ta se shoduje s $\varphi$ v bodech $i+1$ a $i-2$, a s $\varphi^{-1}$ v žádném bodě. Pro všechna $i \in Y$ tedy máme $t(\varphi,\varphi_i^{\pm 1}) = 2$. Z Lemmatu 3.8 plyne, že neexistuje žádné jiné $\psi \in P$, $\psi \neq \varphi_i^{\pm 1}$, které by splňovalo $t(\varphi,\psi) = 2$. Je tedy třeba ukázat, že $t(\varphi_j,\varphi_k) = 2$ pro všechna $j,k \in Y$, $j \neq k$. Dvojici $\{j,k\}$ lze vyjádřit jako $\{i,i+1\}$ nebo jako $\{i,i+2\}$, kde $i \in Y$. Máme

$$\varphi_{i+1} = (i{+}2\ i{-}2\ i{+}1\ i{-}1\ i) \text{ a } \varphi_{i+2} = (i{-}2\ i{-}1\ i{+}2\ i\ i{+}1).$$

Permutace $\varphi_i$ se cs $\varphi_{i+1}$ nikdy neshoduje a s $\varphi_{i+2}$ se shoduje v bodech $i+2$ a $i-2$. Permutace $\varphi_i^{-1}$ se s $\varphi_{i+2}$ neshoduje nikde a s $\varphi_{i+1}$ se shoduje v bodech $i+1$ a $i$. Tvrzení je dokázáno. □

Pro každé $i \in Y$ položme $F_i = \{\{a,b\} \in X;\ i \in \{a,b\}, a \neq b\}$. Dále ať $X' = X \cup \{\infty\}$ a $F_i' = F_i \cup \{\infty\}$, $1 \leq i \leq 5$.

Zvolme $\varphi \in P$ a položme

$$\Phi = \{\psi \in P; (\varphi,\psi) \in \rho\} \quad \text{a} \quad B_\varphi = \{P_\varphi; \varphi \in \Phi\} \cup \left\{F_i';\ i \in Y\right\}.$$

Množinu $B_\varphi$ chápeme jako design na $X'$, tedy jako množinu 11 bloků velikosti 5.

**Lemma 3.7.** *Systém $B_\varphi$ je $2{-}(11,5,2)$ design pro každé $\varphi \in S_5$, $|\varphi| = 5$.*

*Důkaz.* Je-li $i \leq i < j \leq 5$, tak $F_i' \cap F_j' = \{\infty,\{i,j\}\}$. Je-li $\psi,\psi' \in \Phi$ a $P_\psi \neq P_{\psi'}$, tak $|P_\psi \cap P_{\psi'}| = t(\psi,\psi') = 2$. Je-li $i \in Y$ a $\psi \in \Phi$, tak $F_i' \cap P_\psi = \{\{(i,\psi(i)\},\{i,\psi^{-1}(i)\}\}$. Lemma tudíž plyne z Věty 3.5. □

Dva designy se nazývají **izomorfní**, jestliže existuje bijekce jejich nosných množin, která převádí bloky jednoho designu na bloky druhého designu.

Jsou-li $\varphi,\psi \in P$ a $(\varphi,\psi) \in \rho$, tak z definice $B_\varphi$ plyne, že se shoduje s $B_\psi$. Pokud neplatí $(\varphi,\psi) \in \rho$, tak jsou $B_\varphi$ a $B_\psi$ různé designy. Jsou však izomorfní, neboť pokud přejmenujeme prvky $Y$ tak, aby cyklický zápis $\varphi$ či $\psi$ byl roven (1 2 3 4 5), tak vždy dostaneme stejný design.

**Lemma 3.8.** *Až na izomorfismus existuje jediný* $2{-}(11,5,2)$ *design.*

*Důkaz.* Ať $\mathcal{B}$ je takový design na množině $X'$, kde $\infty \in X'$. Označme $F_i'$, $1 \leq i \leq 5$, bloky $\mathcal{B}$, které obsahují bod $\infty$ a položme $F_i = F_i' \setminus \{\infty\}$.

Podle Věty 3.5 je $|F_i \cap F_j| = 1$ kdykoliv $1 \leq i < j \leq 5$. Takových dvojic $(i,j)$ je právě $10 = |X|$. Protože žádné $a \in X$ neleží ve třech různých množinách $F_k$, $k \in Y$, je každé $a \in X$ možné jednoznačně vyjádřit jako $\{a\} = F_i \cap F_j$. Tím dostáváme ztotožnění $X$ s dvoubodovými podmnožinami množiny $Y$. Každý blok $B \in \mathcal{B}$, který neobsahuje $\infty$, poskytuje nějaký graf na $Y$. Pro $i \in Y$ je $|B \cap Y_i| = 2$, takže z každého vrcholu vycházejí právě dvě hrany. To ale znamená, že $B$ je pěticyklus a že ho lze vyjádřit jako $P_\varphi$, kde $\varphi \in P$. Je-li $P_\psi$ nějaký jiný blok $\mathcal{B}$, tak z $|P_\varphi \cap P_\psi| = 2$ plyne $t(\varphi,\psi) = 2$, a proto $\mathcal{B} = B_\varphi$. □

**Důsledek 3.9.** *Až na izomorfismus existuje jediný* $2{-}(11,6,3)$ *design.*

*Důkaz.* Pro $2{-}(11,5,2)$ design $\mathcal{B}$ na $X$ položme $\mathcal{B}' = \{X \setminus B;\, B \in \mathcal{B}\}$. Pokud $B_1$ a $B_2$ jsou dva různé bloky $\mathcal{B}$, tak $|B_1 \cap B_2| = 2$, a proto $(X \setminus B_1) \cap (X \setminus B_2) = X \setminus (B_1 \cup B_2)$ má $11-(5+5-2) = 3$ bodů. $2{-}(11,6,3)$ designy jsou čtvercové, jelikož $3 \cdot 11 \cdot 10 = 11 \cdot 6 \cdot 5$. Podle Věty 3.5 je $\mathcal{B}'$ tedy $2{-}(11,6,3)$ designem. Z každého $2{-}(11,5,2)$ designu lze opačným postupem získat $2{-}(11,6,3)$ design, takže tvrzení je skutečně přímý důsledek Tvrzení 3.10. □

Ať $F$ je komutativní těleso a ať $1 \leq i_1 < \ldots < i_k \leq n$ jsou celá čísla. Zobrazení $F^n \to F^{n-k}$, které z vektoru $(u_1,\ldots,u_n)$ vynechá pozice $i_1,\ldots,i_k$, je jistě homomorfismem vektorových prostorů. Jádro homomorfismu tvoří vektory $(u_1,\ldots,u_n)$ takové, že $u_j = 0$, kdykoliv $1 \leq j < i_1$ nebo $i_k < j \leq n$ nebo $i_s < j < i_{s+1}$ pro nějaké $s$, $1 \leq s < k$. Jinými slovy, v jádru jsou všechny vektory, kde nenulové hodnoty jsou pouze na pozicích $i_1,\ldots,i_k$.

Uvedenému lineárnímu zobrazení budeme říkat **propíchnutí** v pozicích $i_1,\ldots,i_k$.

Je-li $C$ nějaký $[n,k,d]_q$ kód, tak jeho obrazem bude **propíchnutý kód** $C_{i_1,\ldots,i_k}$. Propíchnutý kód je $[n,k-h]_q$ kód, kde $h$ je dimenze prostoru všech kódových slov $C$, které jsou nulové mimo pozice $i_1,\ldots,i_k$.

**Lemma 3.10.** *Ať $C$ je $[n,k,d]_q$ kód, kde $d > 1$. Pak pro každé $i$, $1 \leq i \leq n$, je propíchnutý kód $C_i$ délky $n-1$ a dimenze $k$. Jeho minimální váha je $d-1$ nebo $d$, přičemž první případ nastane, pokud existuje $u \in C$ takové, že $|u| = d$ a $u_i = 0$.*

*Důkaz.* Z $d > 1$ plyne, že žádné kódové slovo nemá váhu 1. Proto se propíchnutím dimenze nezmění. Ať $u \in C$ a ať $u'$ je propíchnuté slovo vzniklé z $u$. Pak $|u'|$ je rovno $|u|$ nebo $|u|-1$. Slovo váhy $d-1$ může v $C_i$ tedy vzniknout jen v popsané situaci. □

**Lemma 3.11.** *Označme $N$ symetrickou matici, která je incidenční maticí* $2{-}(11,6,3)$ *designu. Ať $C$ je samoduální dvojnásobně sudý* $[24,12,8]$ *kód, který*

*obsahuje kódová slova vah* 24 *a* 12. *Každý propíchnutý kód* $C_i$, $1 \leq i \leq 24$, *je permutačně ekvivalentní kódu*

$$\begin{pmatrix} I & \begin{matrix} 1 & \cdots & 1 \end{matrix} \\ & N \end{pmatrix}$$

*přičemž*

$$\begin{pmatrix} & \begin{matrix} 0 & 1 \cdots 1 \end{matrix} \\ I & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \quad N \end{pmatrix}$$

*je kód permutačně ekvivalentní kódu* $C$.

*Důkaz.* Ať $w$ je binární slovo délky 24, které obsahuje samé jedničky. Podle předpokladu existují slova $w'$ a $w''$ váhy 12 taková, že $w = w' + w''$, přičemž $w' \cap w'' = 0$. Můžeme předpokládat, že pozice $i$, ve které propíchneme $C$, splňuje $w'_i = 0$. Zpermutujme pozice tak, aby $w'_1 = w'_2 = \cdots = w'_{12} = 0$ a $w'_{13} = w'_{14} = \cdots = w'_{24} = 1$. Bez újmy na obecnosti nyní můžeme dokonce předpokládat, že $i = 1$. Uvažme všechna $v \in C$ taková, že $v_j = 0$ pokud $1 \leq j \leq 12$. Z $12 = |v| + |w' + v|$ plyne $v \in \{0, w'\}$, neboť $C$ je minimální váhy 8. Propíchnutím $C$ na pozicích 13 až 24 tedy získáme kód délky 12 a dimenze 11. Pokud by prověrková matice tohoto kódu obsahovala alespoň jednu nulu, tak by tento kód obsahoval slovo váhy 1. Pak by bylo možné nalézt $u \in C$ tak, že $|u \cap w''| \equiv 1 \bmod 2$, což je ve sporu s předpokladem $|u \cap w''| \equiv u \cdot w'' = 0 \bmod 2$. Uvažovaná prověrková matice má tedy samé jedničky, takže vzniklý kód je paritní. Je proto možné vytvořit matici, jejíž řádky jsou složeny z kódových slov, která má následující tvar (nuly ve sloupci 13 lze získat odečítáním prvého řádku od všech ostatních).

$$\begin{pmatrix} 0 & \begin{matrix} 0 \cdots 0 \end{matrix} & 1 & \begin{matrix} 1 \cdots 1 \end{matrix} \\ 1 & & 0 & \\ \vdots & I & \vdots & M \\ 1 & & 0 & \end{pmatrix}$$

Tato matice se skládá z řádků lineárně nezávislých, a proto je generující maticí kódu $C$. Vyměníme-li sloupec 1 se sloupcem 13, dostaneme tvar

$$\begin{pmatrix} & \begin{matrix} 0 & 1 \cdots 1 \end{matrix} \\ I & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \quad M \end{pmatrix}$$

Buďte $u_1, \ldots, u_{11}$ řádky matice $M$. Kód $C$ je dvojnásobně sudý, a proto $u_j$ musí mít váhu 2, 6 nebo 10. Současně mají ale váhu alespoň 6. V případě váhy 10 bychom dostali váhu 4 součtem s $w'$. Čili $|u_j| = 6$, kde $1 \leq j \leq 11$. Pro $1 \leq r < s \leq 11$ je ze stejných důvodů $u_r + u_s$ také váhy 6, takže $2|u_r \cap u_s| = |u_r| + |u_s| - |u_r + u_s| = 6$. Vidíme, že $M$ je podle Věty 3.5 incideční maticí $2{-}(11, 6, 3)$ designu. Podle Tvrzení 3.10 lze přehazováním řádků a sloupců převést $M$ na $N$. Pokud výměnu řádků $r$ a $s$ doprovodíme výměnou sloupců $r$ a $s$, získáme generující matici v požadovaném tvaru. □

Uvažme znovu matici $G = (I\ S)$, kde

$$S = \begin{pmatrix} 0 & 1 \cdots 1 \\ 1 & \\ \vdots & N \\ 1 & \end{pmatrix}$$

.

Jde o generující matici nějakého kódu $C$. Každé dva řádky $G$ mají sudý počet společných jedniček, a proto je $C$ kód samoduální. Z Lemmatu 2.10 vyplývá, že je to kód dvojnásobně sudý. Protože matice $S$ je symetrická a $C = C^{\perp}$, je $G' = (S\ I)$ také generující maticí.

Dále dokazujeme, že $d = 8$. Pro spor předpokládejme, že existuje $v \in C$ váhy 4. Ať $A \subseteq \{1, \ldots, 24\}$ jsou ty indexy, že $v_i = 1$ právě pro $i \in A$. Položme $a = |A \cap \{1, \ldots, 12\}|$. Vidíme, že $v$ je součtem $a$ řádků matice $G$ a $4 - a$ řádků matice $G'$. Případ $a \neq 2$ lze zjevně okamžitě vyloučit. Ať $v = u_i + u_j$, kde $u_1, \ldots, u_{12}$ jsou řádky $G$ a $1 \leq i < j \leq 12$. Je-li $i = 1$, je $|v| = 3 + (11 - 6) = 8$ a pro $i \geq 2$ je obdobně $|v| = 2 + 6 = 8$. Minimální váha kódu $C$ je tedy 8.

**Tvrzení 3.12.** *Až na permutační ekvivalenci existuje jediný* $[24, 12, 8]$ *kód, který je dvojnásobně sudý, samoduální a obsahuje kódová slova vah* 12 *a* 24. *Všechny kódy z něj odvozené propíchnutím v jedné pozici jsou vzájemně permutačně ekvivalentní.*

*Důkaz.* Důkaz plyne z úvah předchozího odstavce. □

Kód délky 24 popsaný v Tvrzení 3.14 se nazývá **rozšířený Golayův kód**. Perfektním **binárním Golayovým kódem** se pak nazývá kód délky 23, který z něj získáme propíchnutím.

# 4 Perfektní a MDS kódy

Ať $x \in \mathbb{A}^n$, kde $|\mathbb{A}| = q$. Pro každé $r \geq 1$ je $S(x,r) = \{y \in \mathbb{A}^n;\, d(x,y) \leq r\}$ okolí bodu $x$, které se skládá ze všech vektorů, jež se od $x$ liší v nanejvýš $r$ pozicích. Je-li $C$ kód, který opravuje až $r$-násobné chyby, tak pro $u$, $v \in C$, $u \neq v$ platí $S(u,r) \cap S(v,r) = 0$. Označme $V_q(n,r)$ velikost $S(u,r)$.

**Lemma 4.1.** *Ať $C$ je $(n,h,d)_q$ kód a ať $2r < d$. Potom*

- $h \cdot V_q(n,r) \leq q^n$
- $V_q(n,r) = \sum_{i=0}^{r} (q-1)^r \binom{n}{i}$.

*Důkaz.* Množiny $S(x,r)$, $x \in C$, jsou po dvou disjunktní a mají velikost $V_q(n,r)$. Zjevně $V_q(n,r) - V_q(n,r-1) = (q-1)^r \binom{n}{r}$ pro každé $r \geq 1$, neboť pro změnu na $r$ místech lze vybrat $\binom{n}{r}$ podmnožin a v každé měněné pozici je k dispozici $q-1$ možností. □

Z lemmatu plyne tzv. **Hammingova nerovnost**

$$|C| \cdot V_q\left(n, \left\lfloor \frac{d-1}{2} \right\rfloor\right) \leq q^n,$$

která pro $[n,k,d]_q$ kód má tvar

$$V_q\left(n, \left\lfloor \frac{d-1}{2} \right\rfloor\right) \leq q^{n-k}.$$

Ať $C$ je $q$-ární kód délky $n$ nad abecedou $\mathbb{A}$. Kód $C$ se nazývá **$r$-perfektní**, jestliže $\bigcup_{x \in C} S(x,r) = \mathbb{A}^n$ a $S(x,r) \cap S(y,r) = 0$, pro všechna $x$, $y \in C$, $x \neq y$. Má-li kód $C$ alespoň dva prvky, tak je zřejmé, že je $r$-perfektní právě když Hammingova nerovnost je rovností. V takovém případě zjevně $d = 2r+1$.

Kódu se říká **perfektní**, je-li $r$-perfektní pro nějaké (jednoznačně určené) $r$. Totální kód $\mathbb{A}^n$ je 0-perfektní, jednobodové kódy jsou $n$-perfektní. Perfektní je také opakovací binární kód liché délky $2r+1$. O těchto kódech mluvíme jako o triviálních perfektních kódech.

Hammingův kód má parametry $[n, n-\ell, 3]_q$, kde $n = \frac{q^\ell - 1}{q-1}$ a $\ell \geq 2$. Máme $V_q(n,1) = 1 + (q-1)n = q^\ell$ a $\ell = n - (n-\ell)$, takže vidíme, že Hammingovy kódy jsou také perfektní.

Jedním z největších úspěchů matematické teorie samoopravných kódů je důkaz, že jediné netriviální $r$-pefektní kódy pro $r \geq 2$ mají parametry $[23, 12, 7]_2$ a $[11, 6, 5]_3$. Jsou známy jako (perfektní) **binární Golayův kód** a (perfektní) **ternární Golayův kód**.

Zde se omezíme na důkaz existence a jednoznačnosti binárního Golayova kódu. Pro každý $(n,h,d)_q$ kód $C$ nad $\mathbb{F}_q$ definujme jeho **váhový polynom** $f_C$ jako $\sum f_i x^i \in \mathbb{Z}[x]$, kde $f_i$ udává počet kódových slov váhy $i$. Vidíme, že $f$ je nejvýše

stupně $n$ a že $f_i \leq (q-1)^i \binom{n}{i}$. Je rovněž patrné, že $f_0 \in \{0,1\}$, přičemž $f_0 = 1$ právě když $C$ obsahuje nulový vektor. Je-li $C$ lineární kód váhy $d$, tak $f_0 = 1$ a $f_1 = f_2 = \ldots = f_{d-1} = 0$. Tohoto faktu lze využít pro výpočet váhových polynomů Golayových kódů.

Všimněme si, že $V_2(23,3) = 1+23+\binom{23}{2}+\binom{23}{3} = 1+23(1+11+77) = 2048 = 2^{23-12}$. Každý $[23,12,7]$ kód dává v Hammingové nerovnosti rovnost, a tudíž musí být perfektní.

**Lemma 4.2.** *Váhový polynom* $[23,12,7]$ *kódu je roven* $1 + 253x^7 + 506x^8 + 1288x^{11} + 1288x^{12} + 506x^{15} + 253x^{16} + x^{23}$.

*Důkaz.* Víme, že $f_0 = 1$ a $f_1 = f_2 = \cdots = f_6 = 0$. Uvažme $u \in \mathbb{F}_2^{23}$, $|u| = 4$. Vektor $u$ leží v $S(c,3)$ pro nějaké kódové slovo $c$. Toto slovo je určené jednoznačně a má váhu nejvýše 7. Z $f_4 = f_5 = f_6 = 0$ plyne $|c| = 7$. Kódových slov váhy 7 je $f_7$ a každé slovo váhy 4 je ve vzdálenosti 3 od některého z nich. Proto platí $\binom{7}{3} f_7 = \binom{23}{4}$, odkud $f_7 = 253$. Úvahou o rozmístění slov délky 5 dostaneme $\binom{7}{2} f_7 + \binom{8}{3} f_8 = \binom{23}{5}$, odkud $f_8 = 506$. Při výpočtu $f_9$ je třeba být trochu opatrnější, protože slova váhy 6 lze ze slov váhy 7 obdržet nejen odstraněním jednoho bitu, ale také odstraněním dvou bitů a přidáním třetího na jiné pozici. Máme

$$\left(7 + \binom{7}{2}(23-7)\right) f_7 + \binom{8}{2} f_8 + \binom{9}{3} f_0 = \binom{23}{6}.$$

Snadno odsud vypočítáme, že $f_9 = 0$. Obdobným postupem, který již zde podrobně provádět nebudeme, se spočítají hodnoty $f_i$ pro zbylé indexy $i$, kde $10 \leq i \leq 23$. □

Je-li $C$ binární $[n,k,d]$ kód, tak jeho **rozšířením** rozumíme $[n+1,k]$ kód, kde v přidané pozici (bývá to ta poslední, někdy ale též první) je součet bitů z původních pozic. Rozšířený kód leží v paritním kódu. Pokud již $C$ ležel v paritním kódu, tak v přidané pozici jsou pouze nuly. Proto se při rozšiřování předpokládá, že $C$ obsahuje kódová slova liché délky.

**Lemma 4.3.** *Ať* $C$ *je* $[n,k,d]$ *kód s paritní maticí* $H$*. Rozšířený kód* $C'$ *má pro* $d$ *liché minimální váhu* $d+1$*, zatímco pro* $d$ *sudé se minimální váha nemění. Paritní matici* $H'$ *kódu* $C'$ *lze získat přidáním k* $H$ *nulového sloupce a poté řádku složeného ze samých jedniček.*

*Důkaz.* Pro $u \in C$ ať $u' \in C'$ vznikne z $u$ přidáním paritního bitu. Pak $|u'| = |u| + 1$ právě když $|u|$ je liché. Jinak $|u'| = |u|$. Zbytek je snadný. □

Je-li $C \subseteq \mathbb{F}_q^n$ perfektní kód, tak $u + C$ je také perfektní kód pro každé $u \in \mathbb{F}_q^n$. Proto při zkoumání perfektních kódů $C \subseteq \mathbb{F}_q^n$ lze předpokládat, že $0 \in C$.

**Věta 4.4.** *Až na permutační ekvivalenci existuje jediný* $(23, 4096, 7)$ *kód a jediný* $(24, 4096, 8)$ *kód, které obsahují nulový vektor. Oba jsou lineární. První z nich je perfektní a druhý je samoduální a má váhový polynom* $1 + 759x^8 + 2456x^{12} + 759x^{16} + x^{24}$.

*Důkaz.* Uvažme nějaký $(24, 2048, 8)$ kód $C$, kde $0 \in C$. Propíchnutím vznikne $(23, 2048)$ kód, který má váhu 8 nebo 7. Z Hammingova odhadu plyne, že propíchnutý kód musí být perfektní a že má váhu 7. Váhový kód propíchnutého kódu je popsán v Lemmatu 4.2.

Kdyby v kódu $C$ bylo slovo liché váhy, tak vhodným propíchnutím dostaneme kód s jiným váhovým polynomem, a proto takové slovo existovat nemůže. Všechna slova v propíchnutém kódu tedy mají původ ve slově sudé délky, a proto polynom $1 + 759x^8 + 2456x^{12} + 759x^{16} + x^{24}$ skutečně je váhovým polynomem kódu $C$.

Každý kód $u+C$, kde $u \in C$, má nutně stejný váhový polynom, neboť je rovněž $(24, 4096, 8)$ kódem, který obsahuje 0. Podle Důsledku 2.14 je $C$ samoduálním lineárním dvojnásobně sudým kódem. Víme, že $C$ obsahuje slova váhy 12 i 24, a proto je podle Tvrzení 3.14 určen až na permutační ekvivalenci jednoznačně. Podle téhož tvrzení je až na permutační ekvivalenci určen jednoznačně i každý jeho propíchnutý kód. Takovým kódem přitom musí být každý $(24, 4096, 7)$ kód obsahující 0. Jeho váhový kód totiž známe z Lemmatu 4.2, takže víme, že jeho rozšířením vždy získáme $(24, 4096, 8)$ kód (operaci rozšíření lze zjevně použít i pro nelineární kódy). □

Perfektní kódy jsou největší možné z hlediska Hammingova odhadu. V kapitole 2 jsme definovali MDS kódy. Ty jsou největší možné lineární kódy z hlediska Singletonova odhadu $d \leq n - k + 1$. Podle důsledku 2.8 je $[n, k, d]_q$ kód MDS právě když každých $n - k$ sloupců libovolné prověrkové matice je lineárně nezávislých.

**Tvrzení 4.5.** *Každý $[n, k, d]_q$ kód $C$ je MDS právě když $C^\perp$ je MDS.*

*Důkaz.* Ať $G$ je generující matice kódu $C$. Pak $d < n - k + 1$ právě když $G$ lze zvolit tak, aby v ní existoval řádek, který má $k$ nul. Protože $k = n - (n - k)$ a protože $G$ je podle Důsledku 2.8 prověrkovou maticí kódu $C^\perp$, tak ten nemůže být MDS kódem.

Pokud naopak $C^\perp$ není MDS, tak $C^\perp$ má prověrkovou matici, v níž lze nalézt $k$ lineárně závislých sloupců. Jinými slovy, $C$ má generující matici s $k$ lineárně závislými sloupci. Úpravami na řádcích lze získat jinou generující matici s řádkem, ve kterém oněch $k$ sloupců vytýká samé nuly, odkud $d < n - k + 1$. □

Kód s generující maticí $(1 \cdots 1)$ je zjevně vždy MDS. Jeho doplňkem je paritní kód. MDS kódy libovolné délky vždy existují. Nyní nahlédněme, že toto již neplatí, budeme-li předpokládat, že $3 \leq d \leq n - 1$.

**Tvrzení 4.6.** *Ať $[n, k, d]_q$ kód $C$ je MDS a ať $3 \leq d \leq n - 1$. Potom je $d \leq q$ a $n - q + 1 \leq k \leq q - 1$.*

*Důkaz.* Ať kód $C$ má předpokládané vlastnosti. Z $d = n - k + 1$ plyne $k + 1 = n + 2 - d$, takže podle Tvrzení 4.5 stejné vlastnosti má i kód duální.

A $G = (I\ A)$ je generující matice kódu $C$. Pokud $G$ obsahuje nulu na pozici $(i, j)$ uvnitř $A$ (tedy $j > k$), tak vezmeme v úvahu prvých $k$ sloupců vyjma $i$-tého a přidáme k nim $j$-tý sloupec. Tyto sloupce jsou lineárně závislé, což by byl spor. Matice $A$ obsahuje tedy samé nenuly a má $n-k = d-1 \geq 2$ sloupců. Ať jsou $(a_1, \ldots, a_k)^\mathsf{T}$ a $(b_1, \ldots, b_k)^\mathsf{T}$ po řadě prvý a druhý sloupec matice $A$. Je-li $k \geq q$, tak jistě existují $1 \leq i < j \leq k$, že $a_i/b_i = a_j/b_j$. Pokud těmito sloupci nahradíme $i$-tý a $j$-tý sloupec matice $I$, dostaneme $k$ sloupců, které jsou lineárně závislé. To nelze, a proto $k < q$, $n - k < q$ a $d = n - k + 1 \leq q$. □

**Lemma 4.7.** *Ať $C$ je $[n, k]_q$ kód a ať $G$ je jeho generující matice. Pak $C$ je MDS právě když každých $k$ sloupců $G$ je lineárně nezávislých. Pokud $C'$ obdržíme z $C$ propíchnutím v nejvýše $n - k$ sloupcích, bude $C'$ opět MDS kód.*

*Důkaz.* Prvá část plyne z Tvrzení 4.5 a Důsledku 2.8. Po propíchnutí v nejvýše $n - k$ sloupcích získáme matici, rozměrů $k \times n'$, kde $n' \geq k$ a kde je každých $k$ sloupců lineárně nezávislých. □

# C Cyklické kódy

Ať $C$ je $[n,k]_q$ kód takový, že pro každé $(u_1,\ldots,u_n)\in C$ je také $(u_2,\ldots,u_n,u_1)\in C$. Jinými slovy, kódová slova jsou uzavřena na cyklické posuny. Je přirozené takový kód nazvat **cyklický**.

Strukturu cyklických kódu lze osvětlit, pokud kódová slova budeme chápat jako polynomy. Pro komutativní těleso $F$ ať $F[x]_n$ značí množinu všech $a\in F[x]$ stupně menšího než $n$. Pro $a=\sum a_i x^i\in F[x]$ definujeme $b=\pi_n(a)\in F[x]_n$, $b=b_0+b_1x+\ldots+b_{n-1}x^{n-1}$ tak, že $b_j=\sum_{r\geq 0}a_{j+rn}$. Je snadné vidět, že $\pi_n(a)$ je rovno zbytku po dělení polynomu $a$ polynomem $x^n-1$.

Definujeme-li na $F[x]_n$ sčítání a násobení jako

$$\begin{aligned} a+b &= \pi_n(a+b)\\ a\cdot b &= \pi_n(a\cdot b)\end{aligned}$$

stane se z $F[x]_n$ okruh izomorfní s okruhy $F[x]/(x^n-1)$.

Každý ideál $F[x]$, který obsahuje ideál $x^n-1$, je roven nějakému $(g)$, kde $g$ je jednoznačně určený monický polynom dělící $x^n-1$.

Ideály v $F[x]_n$ mají tvar $\pi_n(gF[x])$. Je-li $x^n-1=gh$, vyjádříme $a\in F[x]$ jako $c\cdot h+b$, kde $\deg b<\deg h$. Pak $\pi_n(ga)=\pi_n(ghc+gb)=\pi_n(gb)=gb$. Proto můžeme vyslovit:

**Tvrzení C.1.** *Buď $F$ komutativní těleso a $n\geq 1$. Pro každý monický dělitel $g$ polynomu $x^n-1$ je množina $C(g)=\{ga;\ a\in F[x],\deg(a)<n-\deg(g)\}$ ideálem okruhu $F[x]_n$ a každý ideál $F[x]_n$ lze takto jednoznačně vyjádřit.*

□

V dalším budeme prvky $\mathbb{F}_q^n$ ztotožňovat s prvky $F_q[x]_n$ tak, aby vektoru $(u_0,u_1,\ldots,u_{n-1})$ odpovídal polynom $u_0+u_1x+u_{n-1}x^{n-1}$. Kódy $C\subseteq\mathbb{F}_q^n$ tedy dále chápeme (také) jako podmnožiny $\mathbb{F}_q[x]_n$.

**Tvrzení C.2.** *Cyklické lineární $q$-ární kódy délky $n$ se shodují s množinami $C(g)$, kde $g$ probíhá všechny dělitele $x^n-1\in\mathbb{F}_q[x]$.*

*Důkaz.* Ať $C\subseteq\mathbb{F}_q[x]_n$ je cyklický lineární kód. Potom je $C$ lineární podprostor $\mathbb{F}_q[x]_n$ a pro každé $u\in C$ je $\pi_n(xu)\in C$. Indukcí dostáváme $\pi_n n(x^iu)\in C$ pro všechna $i\geq 0$, takže $\pi_n(au)=\sum a_i\pi_n(x^iu)\in C$ pro každé $a=\sum a_ix^i\in\mathbb{F}_q[x]$. Vidíme, že $C$ je ideál, a proto lze použít Tvrzení C.1. Naopak je zřejmé, že každý ideál $\mathbb{F}_q[x]_n$ poskytuje lineární cyklický kód. □

**Tvrzení C.3.** *Ať $x^n-1=gh\in\mathbb{F}_q[x]$, kde $g$, $h$ jsou monické polynomy a ať $k=\deg h\geq 1$. Potom $C(g)$ je cyklický $[n,k]_q$ kód. Dále pro $k'=n-k=\deg(g)$ a polynomy*

$$\begin{aligned} g &= g_{k'}x^{k'}+g_{k'-1}x^{k'-1}+\ldots+g_1x+g_0\\ h &= h_kx^k+h_{k-1}x^{k-1}+\ldots+h_1x+h_0\end{aligned}$$

*jsou matice*

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{k'} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{k'-1} & g_{k'} & 0 & \dots & 0 \\ 0 & 0 & g_0 & \cdots & \cdots & g_{k'-1} & g_{k'} & \dots & 0 \\ \vdots & & & \ddots & \ddots & \ddots & & & \vdots \\ 0 & 0 & \dots & 0 & g_0 & \dots & \dots & g_{k'-1} & g_{k'} \end{pmatrix}$$

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \dots & 0 \\ 0 & 0 & h_k & \cdots & \cdots & h_1 & h_0 & \dots & 0 \\ \vdots & & & \ddots & \ddots & \ddots & & & \vdots \\ 0 & 0 & \dots & 0 & h_k & \dots & \dots & h_1 & h_0 \end{pmatrix}$$

*po řadě generující a prověrková matice $C(g)$.*

*Důkaz.* Řádky matice $G$ odpovídají polynomům $g$, $xg$, …, $x^{k-1}g$, takže pro $ga \in C(G)$, kde $\deg a < k$ a $a = \sum a_i x^i$, je $ga = a_0 g + a_1 xg + \cdots + a_{k-1}x^{k-1}g$. Z definice $C(g)$ vyplývá, že $G$ je opravdu jeho generující maticí. Zbývá ověřit, že bodový součin libovolných řádků obou matic dává nulu. Řádky matice $H$ odpovídají polynomům $f$, $xf$, …, $x^{k'-1}f$, kde $f = h_k + h_{k-1}x + \cdots + h_1 x^{k-1} + h_0 x^k$. Bodový součin $x^a g$ a $x^b h$ je v případě $b \geq a$ shodný s bodovým součinem $g$ a $x^\delta h$, kde $b - a = \delta \leq k - 1$, a ten je roven $\sum g_i h_{k-\delta-i}$. V případě $a > b$ je bodový sočin $x^a g$ a $x^b h$ roven bodovému součinu $x^\sigma g$ a $h$, kde $a - b = \sigma \leq k' - 1$, a ten je roven $\sum h_{k-i} g_{i+\sigma}$. Máme $1 \leq k - \delta \leq k$ a $k < k + \sigma \leq k + k' - 1 = n - 1$. Hodnota $\sum_{i+j=r} g_i h_j$ se shoduje s koeficientem $x^r$ v polynomu $x^n - 1 = gh$. Ve všech výše uvažovaných případech je $1 \leq r \leq n - 1$, takže příslušná hodnota je vždy nulová. □

Vidíme, že pro určení struktury cyklických kódů je rozhodující umět rozkládat polynomy $x^n - 1 \in F[x]$, kde $F$ je konečné těleso.

Obecně pro komutativní těleso $F$ máme $x^n - 1 = (x^m - 1)^{p^k}$, pokud $p > 0$ je charakteristika tělesa $F$ a $n = m \cdot p^k$, kde $p$ nedělí $m$. Stačí se tedy zabývat rozklady $x^n - 1$, kde $\operatorname{char} F$ nedělí $n$.

**Tvrzení C.4.** *Ať $F$ je komutativní těleso s prvotělesem $P$. Pro každé $d \geq 1$, kde $char(F)$ nedělí $d$, existuje jednoznačně určený polynom $t_d \in P[x]$, závislý pouze na charakteristice $F$ takový, že pro všechna $n \geq 1$, kde $charF$ nedělí $n$, je $x^n - 1 = \prod_{d|n} t_d$. Pokud se $x^n - 1$ rozkládá v tělese $K \supseteq F$ na kořenové činitele, tak $t_n = \prod(x - \zeta)$, kde $\zeta \in K$ probíhá všechny kořeny $x^n - 1$, které jsou řádu $n$. Přitom $t_n$ je monický polynom stupně $\varphi(n)$, kde $\varphi$ označuje Eulerovu funkci.*

*Důkaz.* Dle definice je $t_1 = x - 1$. Vidíme, že pro $n = 1$ tvrzení platí. Postupujme indukcí. Ať $n > 1$. Protože derivace $x^n - 1$ je rovna $nx^{n-1} \neq 0$, nemá $x^n - 1$ v $K$ vícenásobné kořeny. Množina $R$ všech kořenů $x^n - 1$ v $K$ je konečná podgrupa $K^*$, a proto je cyklická. V cyklické grupě řádu $n$ je právě $\varphi(d)$ prvků

řádu $d$, pro každé $d|n$. Podle indukčního předpokladu je $\prod(x-\xi)$, kde $\xi \in R$ probíhá všechny kořeny řádu $< n$, rovno $\prod_{d|n,d<n} t_d$. Označme tento polynom $r$. Označme $s$ polynom $\prod(x-\zeta)$, kde $\zeta \in R$ probíhá kořeny řádu $n$. Máme $x^n - 1 = rs$, přičemž $r \in F[x]$ je monický. Polynom $s \in K[x]$ se získá tak, že $x^n - 1 \in P[x]$ vydělíme polynomem $r \in P[x]$. Ze znalosti algoritmu dělení plyne, že všechny koeficienty $s$ leží v $P$. Proto $s = t_n \in P[x]$. □

Polynomy $t_n$ se nazývají *cyklotomické* nebo též *kruhové*. Pro $n = p$ prvočíslo je $t_p = 1 + x + \cdots + x^{p-1}$.

**Tvrzení C.5.** *Buď $x^n - 1 \in \mathbb{F}_q[x]$, kde $q$ a $n$ jsou nesoudělné. Polynom $x^n - 1$ se rozkládá v $\mathbb{F}_{q^s}[x]$ na kořenové činitele právě když $q^s \equiv 1$ mod $n$, tedy když $s$ je násobkem řádu $q$ v $\mathbb{Z}_n^*$. Toto nastane právě když $t_n \in \mathbb{F}_q[x]$ má v $\mathbb{F}_{q^s}$ alespoň jeden kořen.*

*Důkaz.* Podmínka je nutná, neboť v tělese, kde se $x^n - 1$ rozkládá na kořenové činitele, existuje podgrupa řádu $n$. Ta tam existuje i v případě, kdy $t_n$ má alespoň jeden kořen. Proto platí, že když má $t_n$ alespoň jeden kořen, tak už se rozkládá na kořenové činitele. Pak $n$ dělí $q^s - 1 = |\mathbb{F}_{q^s}^*|$, což lze jinak vyjádřit jako $q^s \equiv 1 \bmod n$. Polynom $x^{q^s-1} - 1$ se v $\mathbb{F}_{q^s}[x]$ rozkládá na kořenové činitele a $x^n - 1$ ho dělí, pokud $n$ dělí $q^s - 1$. Jde tedy i o podmínku dostačující. □

**Tvrzení C.6.** *Ať $x^n - 1 \in \mathbb{F}_q[x]$, kde $q$ a $n$ jsou nesoudělné. Buď $s$ řád $q$ v $\mathbb{Z}_n^*$. Pak $t_n$ se rozkládá na součin $\varphi(n)/s$ ireducibilních polynomů stupně $s$.*

*Důkaz.* Ať $S$ je množina všech kořenů $x^n - 1 \in \mathbb{F}_{q^s}[x]$, které jsou řádu $n$. Víme, že $t_n = \prod(x-\zeta)$, kde $\zeta \in S$. Je-li $a$ monický ireducibilní dělitel polynomu $t_n$ a $\zeta \in S$ je kořen $a$, tak minimální polynom $m_\zeta \in \mathbb{F}_q[x]$ dělí $a$, a je mu tedy roven. Stačí ukázat, že stupeň $m_\zeta$ je $s$. Stupeň $m_\zeta$ je roven $[\mathbb{F}_q[\zeta] : \mathbb{F}_q]$, což je rovno $s$ právě když $\mathbb{F}_q[\zeta] = K$. Poslední rovnost platí, neboť $s$ je nejmenší číslo takové, že $t_n$ má v $\mathbb{F}_{q^s}$ alespoň jeden kořen. □

Prvek $\zeta$ komutativního tělesa se nazývá **$n$-tá odmocnina z jedné**, pokud $\zeta^n = 1$. Je-li $\zeta$ řádu $n$, hovoříme o **primitivní $n$-té odmocnině z jedné**. Cyklotomický polynom $t_n$, kde $\operatorname{char} F$ nedělí $n$, lze tudíž zapsat jako $\prod(x-\zeta)$, kde $\zeta$ probíhá (ve vhodném rozšíření) všechny primitivní $n$-té odmocniny z jedné. Ireducibilní polynomy dělící $x^n - 1 \in \mathbb{F}_q[x]$ jsou tedy právě všechny minimální polynomy $m_\zeta$, kde $\zeta$ probíhá primitivní $n$-té odmocniny z jedné.

**Lemma C.7.** *Buďte $f$ a $g$ dva dělitelé polynomu $x^n - 1 \in \mathbb{F}_q[x]$. Pak $C(f) \subseteq C(g)$ právě když $g$ dělí $f$. Dále $C(f) \cap C(g) = C(NSN(f,g))$ a $C(NSD(f,g))$ je nejmenší cyklický kód, který obsahuje $C(f)$ i $C(g)$, tedy $C(NSD(f,g)) = C(f) + C(g)$.*

*Důkaz.* Struktura ideálů $\mathbb{F}_q[x]_n$ souhlasí se strukturou ideálů $\mathbb{F}_q[x]$, které obsahují ideál $(x^n - 1)$. Stačí si tedy uvědomit, že je-li $F$ komutativní těleso, tak pro všechna $f, g \in F[x]$ platí $(f) + (g) = (\mathrm{NSD}(f,g))$ a $(f) \cap (g) = (\mathrm{NSN}(f,g))$. □

**Lemma C.8.** *Ať $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$. Položme $u = u_1 + u_2x + \ldots + u_nx^{n-1}$. Nejmenší cyklický kód délky $n$ nad $\mathbb{F}_q$, který obsahuje $(u_1, \ldots, u_n)$, je roven $C(NSD(u, x^n - 1))$.*

*Důkaz.* Jde o nalezení ideálu $\mathbb{F}_q[x]_n$, který obsahuje polynom $u$. Jinak vyjádřeno, hledáme nejmenší ideál $\mathbb{F}_q[x]$, který obsahuje $(u) + (x^n - 1) = \mathrm{NSD}(u, x^n - 1)$. □

**Lemma C.9.** *Ať $C$ je cyklický $[n, k]_q$ kód. Buď $j$, $j' \in \{0, 1, \ldots, n-1\}$ taková, že $jj' \equiv 1 \bmod n$. Sestrojme $C'$ jako množinu všech $\pi_n\left(u\left(x^j\right)\right)$, kde $u(x) = u$ probíhá všechna kódová slova kódu $C \subseteq \mathbb{F}_q[x]_n$. Potom $C'$ je cyklický kód stejné dimenze jako $C$ a je mu permutačně ekvivalentní. Je-li $C = C(f)$, kde $f$ dělí $x^n - 1$, tak $C' = C(NSD(f(x^j), x^n - 1)$.*

*Důkaz.* Pro $C$ platí, že z $u \in C$ plyne $\pi_n(xu) \in C$. Tudíž z $\pi_n(u(x^j)) \in C'$ plyne $\pi_n(x^j u(x^j)) \in C'$. Rotací o $j$ pozic se tedy z kódového slova $C'$ opět stane kódové slovo $C'$. Pokud se tato rotace opakuje $j'$-krát, dostaneme rotaci pouze o jednu pozici, neboť $1 \equiv jj' \bmod n$. Proto je $C'$ uzavřené na cyklické posuny. Je-li $(u_0, u_1, \ldots, u_{n-1}) \in C$, tak $(u_{0j'}, u_{1j'}, \ldots, u_{(n-1)j'}) \in C'$, neboť při počítání indexů a exponentů modulo $n$ máme $u_{ij'}x^i = u_{ij'}x^{ij'j} = u_{ij'}(x^j)^{j'i}$, takže $\sum u_{ij'}x^i = \sum u_{ij'}(x^j)^{j'i} = \sum u_i(x^j)^i = u(x^j)$. Vidíme, že $C'$ je kód permutačně ekvivalentní kódu $C$, a proto musí mít i stejnou dimenzi.

Ať $C = C(g)$. Každý prvek $C$ je sumou lineárních kombinací cyklických posunů $g$. Tudíž $C'$ je sumou lineárních kombinací cyklicých posunů $g(x^j)$. Jde tedy o ideál $\mathbb{F}_q[x]_n$ generovaný polynomem $g(x^j)$, a proto lze použít Lemma C.8. □

**Důsledek C.10.** *Uvažme $m_\zeta \in \mathbb{F}_q[x]$, kde $\zeta$ je primitivní $n$-tá odmocnina z jedné a $NSD(n, q) = 1$. Je-li pro $j > 1$ prvek $\zeta' = \zeta^j$ jiná primitivní odmocnina z jedné a je-li $jj' \equiv 1 \mod n$, tak*

$$m_{\zeta'} = NSD\left(x^n - 1,\, m_\zeta(x^{j'})\right).$$

*Důkaz.* Z Tvrzení C.4 víme, že $m_\zeta$ a $m_{\zeta'}$ jsou stejného stupně. Z Lemmatu C.9 plyne, že takového stupně je i $\mathrm{NSD}(x^n - 1, m_\zeta(x^{j'}))$. Samozřejmě platí, že $m_{\zeta'}$ tento polynom dělí, neboť $(\zeta')^{j'} = \zeta$. □

**Důsledek C.11.** *Ať $f, g \in \mathbb{F}_q[x]$ jsou dva ireducibilní dělitelé $t_n$ a ať $NSD(q, n) = 1$. Pak $C(f)$ a $C(g)$ jsou permutačně ekvivalentní.*

*Důkaz.* Podle Důsledku C.10 máme $f = m_{\zeta'}$ a $g = m_\zeta$ pro vhodná $\zeta$ a $\zeta'$. □

Je dobré si uvědomit, že pokud $f | t_n$, $\mathrm{NSD}(f, q) = 1$ je ireducibilní a $f(\zeta) = 0$, tak $\zeta^q, \ldots, \zeta^{q^{s-1}}$ jsou také kořeny $f$. Hodnotu $s$ volíme jako řád $q$ modulo $n$. Kořeny $f$ jsou tak tvořeny prvky automorfismu $x \mapsto x^q$. Předpoklad $1 = \mathrm{NSD}(n, q)$ je nutný pro to, aby $t_n$ byl polynom bez vícenásobných kořenů. Značná část teorie cyklických kódů předpokladá splnění uvedené podmínky nesoudělnosti.

Podle Lemmatu C.7 je $C(f) + C(g) = C(\mathrm{NSD}(f, g))$. Pokud $C(f) \cap C(g) = 0$, tak je $C(\mathrm{NSD}(f, g)) = C(f) \oplus C(g)$. Ovšem $C(f) \cap C(g) = 0$, pokud $x^n - 1 = \mathrm{NSN}(f, g)$. Poslední uvedená podmínka v případě $\mathrm{NSD}(n, q) = 1$ znamená, že kořeny $f$ a kořeny $g$ pokrývají všechny $n$-té odmocniny z jedné. Rozšířením na více sčítanců pak dostáváme, že $C(\mathrm{NSD}(f_1, \ldots, f_r)) = C(f_1) \oplus \ldots \oplus C(f_r)$, jestliže pro každé $1 \leq j \leq r$ platí, že každá $n$-tá odmocnina z jedná je kořenem $f_j$ nebo kořenem všechny zbylých $f_i$, $i \neq j$. Jsou-li $g_1, \ldots, g_r$ všechny ireducibilní polynomy, které dělí $x^n - 1$, tak tato podmínka bude splněna, pokud položíme $f_i = (x^n - 1)/g_i$, $1 \leq i \leq r$. Můžeme proto vyslovit:

**Tvrzení C.12.** *Ať NSD$(n, q) = 1$ a ať $x^n - 1 = g_1 \cdot \ldots \cdot g_r$ je rozklad na ireducibilní polynomy. Položme $f_i = (x^n - 1)/g_i$. Pak $\mathbb{F}_q^n = C(f_1) \oplus \ldots \oplus C(f_r)$. Současně platí, že $C(f_1), \ldots, C(f_r)$ jsou právě všechny minimální cyklické $q$-ární kódy délky $n$ a $C(g_1), \ldots, C(g_r)$ jsou právě všechny maximální $q$-ární cyklické kódy délky $n$.*

□

**Tvrzení C.13.** *Ať NSD$(n, q) = 1$ a ať $C \subseteq \mathbb{F}_q[x]_n$ je cyklický kód. Ať komutativní těleso $K \supseteq \mathbb{F}_q$ obsahuje $\mathbb{F}_{q^s}$, kde $s$ je řádu $q$ v $\mathbb{Z}_n^*$. Pak $C$ je plně určeno množinou $M$ včech $\zeta \in K^*$, $a(\zeta) = 0$ pro každé $a \in C$. Přitom $C = C(f)$, kde $f = \prod_{\zeta \in M}(x - \zeta)$, a $\zeta \in M$ právě když $m_\zeta$ dělí $f$.*

*Důkaz.* Kód $C$ je roven nějakému $C(f)$. Pokud $\zeta \in M$, tak $m_\zeta$ dělí každé $a \in C$, takže $m_\zeta$ dělí $f$. Je-li naopak $f$ dělitelné $m_\zeta$, tak $C(f) \subseteq C(m_\zeta)$, a tedy $\zeta \in M$. Vidíme, že $M$ splývá jak s množinou kořenů $f$, tak s množinou takových $\zeta \in K$, že $m_\zeta$ dělí $f$. Podmínka $\mathrm{NSD}(n, q) = 1$ je potřebná k tomu, aby $M$ určovalo $f$ jednoznačně. □

**Tvrzení C.14.** *Ať se v komutativním tělese $K \supseteq \mathbb{F}_q$ rozkládá $x^n - 1$ na kořenové činitele. Ať $\xi_1, \ldots, \xi_r \in K$ jsou nějaké $n$-té odmocniny z jedné. Definujme $C$ jako množinu všech $a \in \mathbb{F} - q[x]$. že $a(\xi_1) = \cdots = a(\xi_r) = 0$. Pak $C$ je cyklický kód a $C = \bigcap(C(m_{\xi_i}); 1 \leq i \leq r) = C(NSN(m_{\xi_1}, m_{\xi_2}, \ldots, m_{\xi_r}))$.*

*Důkaz.* Pokud $a \in C$, tak $m_{\xi_i}$ dělí $a$ pro každé $i$, $1 \leq i \leq r$. Proto $C \supseteq C(f)$, kde $f = \mathrm{NSN}(m_{\xi_1}, m_{\xi_2}, \ldots, m_{\xi_r})$. Je-li naopak $a \in C(f)$, tak z $m_{\xi_i} | a$ plyne $a(\xi_i) = 0$. □

# 5 GRS a alternantní kódy

Ať $F$ je komutativní těleso. Označme $\triangle(v_1, \ldots, v_n)$, kde $v_i \in F$, $1 \leq i \leq n$, diagonální matici $D = (d_{ij})$ řádu $n$, ve které $d_{ij} = 0$ pro $i \neq j$ a $d_{ii} = v_i$. Předpokládejme, že všechna $v_i$, $1 \leq i \leq n$, jsou nenulová. Je-li $G$ generující matice kódu $C$ nad $F = \mathbb{F}_q$ a $H$ je jeho prověrková matice, budou $GD$ a $HD^{-1}$ generující a prověrková matice nějakého kódu $C'$. Všimněme si, že $u = (u_1, \ldots, u_n) \in C \Leftrightarrow (u_1 v_1, \ldots, u_n v_n) \in C'$.

Kódy se nazývají **monomiálně ekvivalentní**, pokud lze od jednoho k druhému přejít takovouto úpravou a (ještě navíc) permutací souřadnic.

Ať $n \leq q$ a ať $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ jsou po dvou různé. Uvažme matici

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}.$$

S řádkem 1 asociujeme polynom $1 = x^0$, s řádkem 2 polynom $x$, s řádkem 3 polynom $x^2$ a s řádkem $k$ polynom $x^{k-1}$. Odpovídající řádek můžeme tedy vždy chápat jako vyhodnocení polynomu $x^i$ v bodech $\alpha_1, \ldots, \alpha_n$. Lineární obal řádků $G$ jsou pak vyhodnocení všech polynomů $f$ stupně menšího než $k$ v bodech $\alpha_1, \ldots, \alpha_n$. Všechny polynomy stupně menšího než $k$ tvoří vektorový prostor, řekněme $V_k$, který je dimenze $k$. Polynomy $x^0, \ldots, x^{k-1}$ jsou jeho bází. Zobrazení

$$f \mapsto (f(\alpha_1), \ldots, f(\alpha_n))$$

je lineární zobrazení $V_k \to \mathbb{F}_q^n$. Jeho jádrem jsou polynomy, které na $\alpha_1, \ldots, \alpha_n$ nabývají nulové hodnoty. Nenulový polynom s $n$ nulovými body je stupně alespoň $n$. Pro $n \geq k$ se $V_k$ skládá z polynomů stupně menšího než $n$. To znamená, že uvažované lineární zobrazení má v takovém případě triviální jádro. Je tedy prosté a převádí bázi na bázi. Proto je $G$ pro $k \leq n$ hodnosti $k$.

Předpokládejme $n \geq k$ a uvažme, zda ke $G$, které chápeme jako generující matici, nelze nalézt prověrkovou matici tvaru $HD$, kde $D = \triangle(x_1, \ldots, x_n)$ a

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix}.$$

Bodový součin $i$-tého řádku $G$ a $j$-tého řádku $H$ je roven

$$\alpha_1^{i+j} + \alpha_2^{i+j} + \ldots + \alpha_n^{i+j},$$

takže vlastně chceme zjistit, zda bodový součin $\left(\alpha_1^{i+j}, \ldots, \alpha_n^{i+j}\right)$ s $(x_1, \ldots, x_n)$

je roven nule, pokud $0 \leq i+j \leq n-2$. Hledáme tedy řešení následující soustavy

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \cdots & \alpha_n^{n-2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

.

Takové řešení existuje, neboť zde vystupuje matice $(n-1)\times n$, která je hodnosti $n-1$. Ať $(x_1, \ldots, x_n)$ je nějaké netriviální řešení. Pokud by pro některé $i$, $1 \leq i \leq n$, platilo $x_i = 0$, tak vypuštěním hodnoty $x_i$ a vypuštěním $i$-tého sloupce dostaneme součin $Ay^T = 0$, kde $y = (x_1, \ldots, x_{i-1}, x_{i+1}, x_n) \neq 0$ a $A$ je čtvercová regulární matice řádu $n-1$. To není možné, a proto všechna $x_i$ jsou nenulová. Tedy $H \cdot \triangle(x_1, \ldots, x_n)$ je prověrkovou maticí $C$.

Ať $v_1, \ldots, v_n \in \mathbb{F}_q^*$ a ať $1 \leq k \leq n$. Pokud $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q^*$ jsou po dvou různá, tak se kód s prověrkovou maticí $H\triangle(v_1, \ldots, v_n)$ nazývá **zobecněný Reed-Solomonův kód** (GRS kód) s **lokátory** $\alpha_1, \ldots, \alpha_n$ a **multiplikátory** $v_1, \ldots, v_n$.

**Tvrzení 5.1.** *Buďte $1 \leq k \leq n \leq q$. Ať $C$ je GRS kód dimenze $k$ s lokátory $\alpha_1, \ldots, \alpha_n$ a multiplikátory $v_1, \ldots, v_n$. Pak existují $v_i' \in \mathbb{F}_q^*$, $1 \leq i \leq n$, že $C^\perp$ je GRS kód s lokátory $\alpha_1, \ldots, \alpha_n$ a multiplikátory $v_1', \ldots, v_n'$. Kódy $C$ i $C'$ jsou MDS kódy.*

*Důkaz.* Tvrzení plyne z předchozích úvah. Je nutné si uvědomit, že každá $k \times k$ podmatice matice $G$ je podle dokázaného hodnosti $k$, takže je regulární. GRS kódy jsou proto MDS. □

Součástí definice GRS kódu je předpoklad nenulovosti lokátorů $\alpha_i$. Tento předpoklad jsme však v úvahách výše nijak nepoužili. Tvrzení 5.1 proto platí i tehdy, je-li některý lokátor nulový.

Některé GRS kódy mají zvláštní označení. Pokud $n = q-1$, nazýváme GRS kód **primitivní**. V takovém případě $\alpha_1, \ldots, \alpha_n$ procházejí celou množinu $\mathbb{F}_q^*$.

**Normalizovaný GRS kód** má všechny multiplikátory rovny jedné, takže k žádné úpravě základní matice nedochází.

O **GRS kódu v užším slova smyslu** hovoříme, pokud $v_j = \alpha_j$, $1 \leq j \leq n$. V takovém případě je prověrková matice tvaru

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k} & \alpha_2^{n-k} & \cdots & \alpha_n^{n-k} \end{pmatrix}.$$

**Konvenční (běžné) RS kódy** (či pouze RS kódy) jsou určeny prvkem $\alpha \in \mathbb{F}_q^*$ řádu $n$, kde $n$ dělí $q-1$. Předpokládá se, že $\alpha_j = \alpha^{j-1}$ a $v_j = \alpha^{b(j-1)}$, kde $b \geq 0$ je celé číslo.

Vidíme, že RS kódy mají prověrkovou matici

$$H = \begin{pmatrix} 1 & \alpha^b & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{b+d-2} & \cdots & \alpha^{(n-1)(b+d-2)} \end{pmatrix},$$

kde se místo $n-k$ píše $d-1$ (připomeňme si, že se jedná o MDS kód). Případy $b=0$ a $b=1$ dávají matice

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{d-2} & \cdots & \alpha^{(d-2)(n-1)} \end{pmatrix} \text{ a } \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{d-1} & \cdots & \alpha^{(d-1)(n-1)} \end{pmatrix}.$$

Kódy generované maticemi se v souladu s obecnou terminologií nazývají **RS kódy v normalizovaném tvaru** a RS kódy v užším slova smyslu.

Ať $C'$ je nějaký $[n,k,D]$ kód nad $\mathbb{F}_{q^s}$. Kód $C'$ je tedy lineární podprostor $(\mathbb{F}_{q^s})^n$. Víme, že $\mathbb{F}_{q^s}$ lze chápat jako vektorový prostor nad $\mathbb{F}_q \subseteq \mathbb{F}_{q^s}$, a to dimenze $s$. Při takovém pojetí se z $(\mathbb{F}_{q^s})^n$ stává vektorový prostor nad $\mathbb{F}_q$ dimenze $sn$. V tomto prostoru leží $(\mathbb{F}_q)^n$ jako podprostor. Z kódu $C'$ můžeme odvodit $q$-ární kód $C = C' \cap (\mathbb{F}_q)^n$. Říkáme mu **reziduální** $q$-ární kód kódu $C$.

Reziduální kódy GRS kódu se nazývají **alternantní kódy**. Jejich podtřídou jsou BCH kódy, což jsou reziduální kódy RS kódu. Označení GRS kódu jako primitivního, normalizovaného nebo v užším slova smyslu se přenáší i na alternantní a BCH kódy.

Koncept reziduálního kódu přináší zejména odhad jeho minimální vzdálenosti. Okamžitě vidíme, že kód $C$ je délky $n$, a že jeho minimální vzdálenost $d$ je alespoň $D$. Pokud $k = \dim C$ je dostatečně velké, můžeme získat kód příznivých parametrů, jehož přímá konstrukce by byla obtížná.

Tentýž kód je obecně vzato možno získat jako reziduální kód více způsoby. Je-li z kontextu patrné, jakou reziduální konstrukcí jsme kód $C$ získali, nazýváme $D$ jeho **zaručenou vzdáleností** (nejde o přesný překlad anglického termínu *designed distance*, ale o volbu sousloví, které roli $D$ co nejlépe vystihuje).

Jsou situace, kdy známe $D$, avšak zjištění $d \geq D$ je obtížné. Stejně tak není vždy snadné zjistit dimenzi $k$ kódu $C$. Cílem samozřejmě je získat $k$ co největší. Následující odhad dokážeme snadno, ovšem ten hodnotu $k$ zpravidla značně podceňuje.

**Lemma 5.2.** *Ať $C$ je $[n,k]_q$ alternantní kód zaručené vzdálenosti $D$, který je sestrojen jako reziduální z GRS kódu $C'$ nad $\mathbb{F}_{q^s}$. Potom $k \geq n - s(D-1)$.*

*Důkaz.* Označme $K$ dimenzi kódu $C'$. Víme, že $C'$ je MDS kód parametrů $[n, K, D]$, takže $D = n - K + 1$. Nerovnost $k \geq n - s(n - K)$ zapíšeme jako $n - k \leq s(n - K)$. Protože $n - k$ je počet řádků prověrkové matice kódu $C$, tak k důkazu nerovnosti stačí nalézt takovou matici $M$ rozměrů $(n - K)s \times n$, že $u \in C$ právě když $Mu^{\mathsf{T}} = 0$.

Zvolme nějakou bázi $(\beta_1, \ldots, \beta_s)$ tělesa $\mathbb{F}_{q^s}$ nad $\mathbb{F}_s$. Uvažme bodový součin $c \cdot u$ nějakých vektorů $c = (\gamma_1, \ldots, \gamma_n) \in \mathbb{F}_{q^2}^s$ a $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$. Ať $\gamma_j = \sum_{i=1}^{s} a_{ji}\beta_i$, kde $a_{ji} \in \mathbb{F}_q$, $1 \leq j \leq n$. Položme $a_i = (a_{1i}, \ldots, a_{ni})$. Pak $c \cdot u = \sum_{j=1}^{n} \sum_{i=1}^{s} c_j a_{ji} \beta_i = \sum_{i=1}^{s} (\sum_{j=1}^{n} c_j a_{ji}) \beta_j = \sum_{i=1}^{s} (c \cdot a_i)\beta_i$. Vidíme, že $c \cdot u = 0$ právě když $c \cdot a_i = 0$ pro všechna $i$, $1 \leq i \leq s$.

Buď nyní $H$ prověrková matice kódu $C'$ s řádky $c_1, \ldots, c_{n-K}$. Každý řádek $c_r = (\gamma_1, \ldots, \gamma_n)$ nahradíme $s$ řádky $a_1, \ldots, a_s$ jakoby bylo $c = c_r$. Zkonstruovanou matici označíme $M$. Protože $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ padne do $C'$ právě když $Hu^{\mathsf{T}} = 0$, lze podle předchozího totéž ověřit vztahem $Mu^{\mathsf{T}} = 0$. □

# D BCH kódy a QR kódy

Připomeňme, že RS kód $C$ dimenze $k$ má prověrkovou matici $H = (\alpha^{ij})$, kde $0 \le j \le n-1$ a kde $i$ probíhá od $b$ do $b+d-2$, přičemž $d = n-k+1$. Průběh $i$ se přitom chápe modulo $n$, takže za $i = n-1$ následuje $i = 0$. Prvek $\alpha \in \mathbb{F}_q$ je primitivní $n$-tou odmocninou z jedné.

Uvažme řádek $u = (1, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(n-1)i})$ matice $H$. Vidíme, že jeho cyklický posun $(\alpha^{(n-1)i}, 1, \alpha^i, \ldots, \alpha^{(n-2)i})$ je roven $\alpha^{-i}u$, takže každý RS-kód je cyklický (platí vlastně i něco silnějšího – existuje prověrková matice, kde cyklické posunutí každého řádku je jeho lineárním násobkem). Přitom $a = \sum a_j x^j$ padne do $C$ právě když pro každé $i$ z daného (cyklického) intervalu je $\sum a_j \alpha^{ij} = 0$, čili $\alpha^i$ je kořenem $a$. Stupeň generujícího polynomu je roven dimenzi prověrkové matice (to platí v každém cyklickém kódu). Každý řádek matice $H$ udává jeden kořen generujícího polynomu, takže ten musí být roven $(x-\alpha^b)\cdots(x-\alpha^{b+d-2})$.

**Tvrzení D.1.** *Ať $C$ je $[n,k,d]_q$ RS kód s generující maticí $(\alpha^{ij})$, kde $i$ probíhá od $b$ do $b+d-2$. Pak $C = C((x-\alpha^b)\cdots(x-\alpha^{b+d-2}))$ a $C^\perp = C((x-\alpha^{1-b})\cdots(x-\alpha^{k-b}))$.*

*Důkaz.* Prvou část tvrzení jsme již dokázali. Víme, že pro $C = C(g)$ je $C^\perp = C(h(x^{-1}))$, kde $gh = x^n - 1$. V našem případě se $x^n - 1$ rozkládá na $\prod_{i=0}^{n-1}(x-\alpha^i)$. Obecně platí, že jsou-li $\alpha_1, \ldots, \alpha_{d-1}$ kořeny $g$, musí mít $h$ kořeny $\alpha_d^{-1}, \ldots, \alpha_n^{-1}$ tak, aby $\{\alpha_1, \ldots, \alpha_n\} = \{\alpha^i;\ 0 \le i < n\}$. Probíhá-li $i$ od $1-b$ do $k-b = n-d+1-b$, tak $-i$ probíhá od $d+b-1$ do $b-1$. Proto je generující polynom kódu $C^\perp$ zvolen správně. □

**Důsledek D.2.** *Duální kód RS kódu je opět RS kód. Duální kód normalizovaného RS kódu je RS kód v užším smyslu, a naopak.*

*Důkaz.* Podle definice má normalizovaný RS kód generující polynom $(x-1)\cdots(x-\alpha^{n-k-1})$. Jeho duální kód má podle Tvrzení D.1 generující polynom $(x-\alpha^k)(x-\alpha^{k-1})\cdots(x-\alpha)$, což je generující polynom RS kódu v užším smyslu. Na základě Tvrzení D.1 je zřejmý i zbytek. □

**Tvrzení D.3.** *Ať $C$ je BCH kód nad $\mathbb{F}_q$ určený RS-kódem s generujícím polynomem $(x-\alpha^b)\cdots(x-\alpha^{b+d-2})$, kde $\alpha \in \mathbb{F}_{q^s}$ je primitivní $n$-tá odmocnina z jedné. Pak $C$ je cyklický kód nad $\mathbb{F}_q$ a $C = C(\mathrm{NSN}(m_{\alpha^b}, \ldots, m_{\alpha^{b+d-2}}))$.*

*Důkaz.* Polynom $a \in \mathbb{F}_q[x]_n$ leží v $C$, pokud hodnoty $a(\alpha^b), \ldots, a(\alpha^{b+d-2})$ jsou rovny nule. □

Charakterizace BCH kódů jejich nulami nám v konkrétních případech umožňuje dopočítat jejich přesnou dimenzi. Protože kodimenze je rovna stupni generujícího polynomu, stačí znát počet kořenů generujícího polynomu určeného Tvrzením D.3. Každý ireducibilní polynom s kořenem $\alpha^i$ má množinu všech kořenů shodnou s $\{\alpha^{iq^r};\ r \ge 0\}$. Proto je kodimenze kódu $C$ rovna velikosti podmnožiny $\mathbb{Z}_n$,

která vznikne, jestliže ke každému $i \in \{b, \ldots, b+d-1\} \subseteq \mathbb{Z}_n$ přidáme (modulo $n$) všechny hodnoty $iq^r$, $r \geq 0$.

Další významnou třídou kódů, kterými se budeme zabývat, jsou takzvané QR-kódy, kde QR je zkratkou od Quadratic residue (kvadratický zbytek).

Tyto kódy jsou binární a definují se pro lichou prvočíselnou délku $n$. Zvolíme nějakou primitivní $n$-tou odmocninu z jedné a označíme ji $\alpha$. Víme, že $x^n - 1 = (x-1)\prod_{i=1}^{n=1}(x-\alpha^i)$. Grupu $\mathbb{Z}_n^* = \{i;\, 1 \leq i \leq n-1\}$ můžeme vyjádřit jako disjuktní sjednocení $R \cup S$, kde $i \in R$ právě když $i = j^2$ pro nějaké $j \in \mathbb{Z}_n^*$, tedy když $i$ je kvadratický zbytek modulo $n$. Těchto zbytků je $(n-1)/2$, takže polynomy

$$g_0 = \prod_{i \in R}(x - \alpha^i) \text{ a } g_1 = \prod_{i \in S}(x - \alpha^i)$$

jsou stupně $(n-1)/2$ a splňují $x^n - 1 = (x-1)g_0g_1$.

Pro $n$-tou odmocninu z jedné platí, že je kořenem polynomu $g_0(x^j)$, kde $jj' \equiv 1 \bmod n$, právě když je tvaru $\alpha^{ij'}$, $i \in R$. Proto $g_0(x^j) \equiv \prod(x - \alpha^{ij'}) \bmod x^n - 1$, takže

$$g_0(x^j) \equiv g_0 \text{ pro } j \in R \text{ a } g_0(x^j) \equiv g_1 \text{ pro } j \in S.$$

Z $g_0 \in \mathbb{F}_2[x]$ plyne $g_1 \in \mathbb{F}_2[x]$, a pak jsou kódy $C(g_0)$ a $C(g_1)$, jak vidíme, permutačně ekvivalentní. Aby $g_0$ leželo v $\mathbb{F}_2[x]$, musí být jeho kořeny uzavřeny na Frobeniův automorfismus. Jinými slovy, je-li $\alpha$ kořen $g_0$, musí být i $\alpha^2$ také kořenem $g_0$. To nastane právě když $2 \in R$, což platí právě když $n \equiv \pm 1 \bmod 8$.

Dále budeme uvažovat pouze případ, kdy $n$ je prvočíslo tvaru $8\ell - 1$ nebo $8\ell + 1$. Za QR kód budeme považovat cyklický kód $C(g_0)$. Ten je ovšem závislý na volbě $\alpha$ – při jiné volbě $\alpha$ dostaneme $C(g_1)$. To je určitá formální nedůslednost, která však nevede k obtížím, neboť $C(g_0)$ a $C(g_1)$ jsou permutačně ekvivalentní. Je zřejmé, že vždy jde o $[n, (n+1)/2]$ kód, neboť $g_0$ je stupně $(n-1)/2$.

*Rozšířeným QR-kódem* $\bar{C}$ budeme rozumět rozšíření QR kódu o bit paritní kontroly. Vidíme, že $\bar{C}$ je $[n+1, (n+1)/2]$ kód.

**Tvrzení D.4.** *Rozšířený QR kód je samoduální právě když* $n \equiv -1 \bmod 8$.

*Důkaz.* Ze vztahu $C((x+1)g_0) = C(x+1) \cap C(g_0)$ plyne, že $C((x+1)g_0)$ je v $C(g_0)$ podprostor indexu 2 (jinými slovy, $C((x+1)g_0)$ je nadrovinou $C(g_0)$). Přidávaný paritní bit je roven nule právě když kódové slovo leží v $C((x+1)g_0)$, protože $C(x+1)$ se skládá právě ze všech slov sudé váhy.

Všechna kódová slova $\bar{C}$ musí být proto po odstranění přidaného paritního bitu kolmá na všechny vektory $C((x+1)g_0)$. To vlastně znamená $C(g_0) \subseteq C((x+1)g_0)^\perp$, což z důvodů dimenze je totéž jako $C(g_0) = C((x+1)g_0)^\perp$. Z $x^n - 1 = (x+1)g_0g_1$ plyne, že kód $C((x+1)g_0)^\perp$ je generován polynomem $g_1(x^{-1})$. Tento kód má být roven $C(g_0)$, což znamená, že $g_0(x)$ a $g_1(x^{-1})$ mají mít stejné kořeny. To ovšem nastane právě pro $-1 \in S$. Víme, že $-1$ je

nečtverec modulo $n$ právě když $n \equiv 3 \bmod 4$. Podmínka dokazovaného tvrzení je tedy nutná.

Uvažme nyní kódová slova $u, v \in C(g_0)$ a označme $\bar{u}$ a $\bar{v}$ jejich rozšíření o paritní bit. Předpokládejme, že $n \equiv -1 \bmod 8$, tedy že $C((x+1)g_0)^\perp = C(g_0)$. Pokud $u$ nebo $v$ padne do $C((x+1)g_0)$, tak z nulovosti paritního bitu plyne $\bar{u} \cdot \bar{v} = u \cdot v = 0$. Ať $u, v \in C(g_0) \setminus C((x+1)g_0)$. Pak $\bar{u} \cdot \bar{v} = u \cdot v + 1$, takže potřebujeme dokázat $u \cdot v = 1$.

Protože neplatí $\langle u \rangle \subseteq C(g_0)^\perp$, tak neplatí ani $C(g_0) \subseteq \langle u \rangle^\perp$. To znamená, že nadrovina $\langle u \rangle^\perp$ vytíná v $C(g_0)$ také nadrovinu. Tato nadrovina je rovna $C((x+1)g_0)$, neboť $C((x+1)g_0) = C(g_0)^\perp \subseteq \langle u \rangle^\perp$. Tudíž $v \notin \langle u \rangle^\perp$, a proto $u \cdot v = 1$. □

Parita kódových slov cyklických kódů respektuje operace sčítání a násobení polynomů. Pro $a \in \mathbb{F}_2[x]$ počet nenulových koeficientů označíme (na chvíli) $|a|$. Máme $|a| \equiv a(1) \bmod 2$, a proto je $a \mapsto |a| \bmod 2$ homomorfismem $\mathbb{F}_2[x] \to \mathbb{F}_2$. Jeho jádrem je ideál $(x+1) \supseteq (x^n+1)$, a proto $a \mapsto |a| \bmod 2$ je i homomorfismem $\mathbb{F}_2[x]_n \to \mathbb{F}_2$.

Ze vzorce pro násobení polynomů $ab = \sum a_i b_j x^{i+j}$, kde $a = \sum a_i x^i$ a $b = \sum b_j x^j$, vyplývá $|ab| \leq |a| \cdot |b|$. Tento vztah platí nad libovolným tělesem $F$, nejen nad $\mathbb{F}_2$. Také samozřejmě platí i pro okruh $F[x, x^{-1}]$.

Pokud $b = a(x^{-1})$, tak v součinu $ab$ figurují členy $a_i a_i x^{i-i} = a_i^2$. Z počtu $|a| \cdot |b|$ nenulových součinů $a_i b_j$ jich pak $|a|$ dává $a_i a_i x^{i-i} = a_i^2 x^0$. Proto

$$|a(x) \cdot a(x^{-1})| \leq |a|^2 - |a| + 1.$$

Tyto jednoduché úvahy tvoří základ důkazu následujícího pozorování.

**Lemma D.5.** *Ať je $a \in C(g_0)$ a ať $d = |a|$ je liché. Potom $d^2 \geq n$. Je-li $n \equiv 7 \bmod 8$, tak dokonce $d^2 - d + 1 \geq n$.*

*Důkaz.* Polynomy $C(g_0)$ a $C(g_1)$ jsou permutačně ekvivalentní. Proto v $C(g_1)$ existuje kódový polynom $b$, který je také váhy $d$. Polynom $ab$ je násobek polynomu $g_0 g_1 = 1 + x + x^2 + \cdots + x^{n-1}$. Kód $C(1 + \cdots + x^{n-1})$ se skládá ze dvou kódových slov, nenulové z nich je rovno $w = (1, \ldots, 1)$. Víme, že $|\pi_n(ab)| \equiv |a| \cdot |b| \bmod 2$. Tudíž $|\pi_n(ab)| \equiv d^2 \equiv 1 \bmod 2$, takže $\pi_n(ab) = w$. Polynom $ab$ má tedy alespoň $n$ nenulových koeficientů, a proto $d^2 \geq n$.

V případě $n \equiv -1 \bmod 8$ je $C(g_1)$ generováno $g_0(x^{-1})$, takže za $b$ lze zvolit $a(x^{-1})$. Z toho plyne odhad $d^2 - d + 1 \geq n$. □

Odhady $d^2 \geq n$ a $d^2 + d - 1 \geq n$ lze použít jako odhady minimální vzdálenosti QR kódu $C(g_0)$, pokud se podaří ověřit:

**Lemma D.6.** *Minimální váha QR-kódu je lichá.*

Podrobný důkaz tohoto lemmatu zde provádět nebudeme a omezíme se na jeho hlavní myšlenku. Pracuje se s rozšířeným kódem $\bar{C}$, o kterém se dokáže, že jeho grupa automorfismů je tranzitivní (automorfismy jsou zde permutační ekvivalence kódu $\bar{C}$ sama se sebou). To znamená, že pro libovolná $i, j \in \{1, \ldots, n+1\}$ existuje $\varphi \in S_{n+1}$ takové, že $\varphi(i) = j$ a současně $(u_{\varphi(1)}, \ldots, u_{\varphi(n+1)}) \in \bar{C}$ kdykoliv $(u_1, \ldots, u_{n+1}) \in \bar{C}$. Je-li $(u_1, \ldots, u_n) \in C(g_0)$ slovo minimální váhy, a ta je sudá, zvolíme $\varphi$ tak, aby $\varphi(n+1) = i$, kde $u_i = 1$. Ze sudosti váhy plyne $u_{n+1} = 0$, takže $(u_{\varphi(1)}, \ldots, u_{\varphi(n+1)})$ má na prvých $n$ pozicích váhu o jedničku menší, což je spor s volbou $(u_1, \ldots, u_n)$.

Ze vztahu $d^2 - d + 1 \geq n$ a informace, že $d$ je číslo liché, dostáváme pro $n = 7$ odhad $d \geq 3$ a pro $n = 23$ odhad $d \geq 7$. Z důvodů Hammingovy nerovnosti musí platit $d = 3$ a $d = 7$. Vidíme, že základní Hammingův kód a perfektní binární Golayův kód je možné získat jako QR kódy, a tedy jako kódy cyklické.

# 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.

# 7 Hadamardovy matice a kódy, a něco odhadů.

V kapitole 3 jsme konstruovali $2{-}(11,5,2)$ design. Pro $2=\lambda-1$ bude $3=\lambda$, $5=2\lambda-1$ a $11=4\lambda-1$, takže $2{-}(11,5,2)$ design je příkladem $2{-}(4\lambda-1,2\lambda-1,\lambda-1)$ designu. Takovým designům se říká *Hadamardovy*. Otázka je, zda existují i pro jiné hodnoty $\lambda$. Pro $\lambda=2$ dostáváme parametry $(7,3,1)$, čemuž vyhovuje Fanova rovina. Další příklady uvedeme později. Nejprve se budeme zabývat obecnými vlastnostmi takových designů.

Standardní rovnost $r(k-1)=(v-1)\lambda$ má v našem případě tvar $r(2\lambda-2)=(4\lambda-2)(\lambda-1)$, odkud $r=2\lambda-1$, takže rovnost $kb=vr$ implikuje $v=b=4\lambda-1$. Vidíme, že Hadamardovy designy jsou čtvercové. Každé dva různé bloky se protínají právě v $\lambda-1$ bodech.

Uvažme incidenční matici $M$ nějakého $2{-}(4\lambda{-}1,2\lambda{-}1,\lambda{-}1)$ designu. Dva její různé řádky mají společných $\lambda-1$ jedniček a $(4\lambda-1)-2(2\lambda-1)+(\lambda-1)=\lambda$ nul. Vytvořme novou matici $H$ tak, že k $M$ přidáme řádek a sloupec složený ze samých jedniček a současně všechny nuly změníme na minus jedničky. Ve vzniklé matici se dva různé řádky $u$ a $v$ shodují právě na $2\lambda$ místech. Uvážíme-li jejich bodový součin $u\cdot v$, vidíme, že shody dávají v jednotlivých pozicích $+1$ a neshody $-1$, takže $u\cdot v=0$. Jinými slovy, $HH^{\mathsf{T}}=nI$, kde $n=4\lambda$.

Každá matice $H$ řádu $n$, která splňuje $HH^{\mathsf{T}}=nI$ a obsahuje pouze hodnoty $+1$ a $-1$, se nazývá *Hadamardova*. Jsou-li její prvý řádek a prvý sloupec složeny toliko z hodnot $+1$, hovoříme o Hadamardově matici v *normalizovaném* tvaru. Hadamardovy designy indukují, jak jsme nahlédli, právě takové Hadamardovy matice.

Rovnost $HH^{\mathsf{T}}=nI$ implikuje, že každé dva různé řádky mají stejný počet shod a neshod. Číslo $n$ tedy musí být sudé, pokud $n>1$. Vynásobíme-li libovolný sloupec hodnotou $-1$, počet neshod se nemění. Rovnost $HH^{\mathsf{T}}=nI$ rovněž zjevně zůstává v platnosti, pokud vynásobíme řádek hodnotou $-1$. Každou Hadamardovu matici proto lze převést do normalizovaného tvaru.

Ať $H$ je taková matice řádu $2h\geq 4$. Ať $u$ a $v$ jsou dva její různé řádky, přičemž žádný z nich ať není prvý řádek matice. Každý z nich v bodovém součinu s prvým řádkem dává nulu. Protože prvý řádek je složen ze samých jedniček, tak $u$ i $v$ musí obsahovat $h$ hodnot $+1$ a $h$ hodnot $-1$. Ať se shodují v $\lambda$ společných hodnotách $+1$. Potom je přesně $h-\lambda$ sloupců, ve kterých je v $u$ hodnota $+1$ a ve $v$ hodnota $-1$. Stejně je i sloupců, kde $v$ má $+1$ a $u$ má $-1$. Proto se $u$ a $v$ neshodují právě v $2(h-\lambda)$ pozicích. Počet těchto pozic musí být ale také roven $h$, neboť $u\cdot v=0$. Vidíme, že $h=2\lambda$ je číslo sudé, a že počet společných $+1$ (a podobně i $-1$) je přesně $\lambda$.

Pro Hadamardovu matici $H$ (ne nutně normalizovanou) položme $H_1=\frac{1}{\sqrt{n}}H$. Pak $H_1H_1^{\mathsf{T}}=I$, takže $H_1^{\mathsf{T}}=H_1^{-1}$, odkud $H_1^{\mathsf{T}}H_1=I$ a $H^{\mathsf{T}}H=nI$. Vidíme, že transpozicí vznikne z Hadamardovy matice opět matice Hadamardova. V každém sloupci (kromě prvního) normalizované Hadamardovy matice řádu $2h>4$ je tedy právě $h$ hodnot $+1$.

Matice (1) a $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ jsou Hadamardovy. Hadamardovy matice vyšších řádů lze odvodit, jak dokazuje následující tvrzení, z Hadamardových designů. Odvozením přitom rozumíme výše popsaný postup, kdy se z incidenční matice $M$ vytváří matice $H$, kterou lze dále upravovat násobením řádků a sloupců hodnotou $-1$.

**Tvrzení 7.1.** *Každou Hadamardovu matici řádu $n \geq 3$ lze odvodit z nějakého $2{-}(4\lambda-1, 2\lambda-1, \lambda-1)$ designu, kde $4\lambda = n$.*

*Důkaz.* Ať $H$ je normalizovaná Hadamardova matice řádu $n \geq 3$. Výše jsme již ukázali, že $n = 4\lambda$, přičemž každý řádek kromě prvého obsahuje $2\lambda$ hodnot $+1$ a $2\lambda$ hodnot $-1$. Dva takové různé řádky mají hodnotu $+1$ právě na $\lambda$ společných pozicích.

Odstraňme nyní prvý řádek a prvý sloupec a nahraďme všechny výskyty hodnoty $-1$ hodnotou 0. Získanou matici označme $M$. Je to incidenční matice designu s bloky délky $2\lambda - 1$. Dva různé bloky mají společných $\lambda - 1$ bodů, protože odpovídající řádky mají společných $\lambda$ jedniček, a každý bod leží v $2\lambda - 1$ blocích, protože odpovídající sloupec obsahuje právě $2\lambda$ jedniček. Podle Věty 3.5 proto jde o $2{-}(4\lambda-1, 2\lambda-1, \lambda-1)$ design. □

Je-li $H$ Hadamardova matice, tak lze snadno nahlédnout, že $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ je rovněž Hadamardova matice. Maticím takto postupně odvozovaným z matice $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ se říká *Sylvestrovy $H$-matice*. Mají řád $2^m$, $m \geq 1$. Lze je snadno vyjádřit i přímo. Pokud řádky i sloupce číslujeme od 0 do $2^k - 1$, tak pro $j = \sum \varepsilon_i 2^i$ a $j' = \sum \varepsilon'_i 2^i$ v buňce $(j, j')$ leží hodnota $(-1)^{\sum \varepsilon_i \varepsilon_{i'}}$. Sylvestrova $H$-matice řádu $2^k$ se tak vlastně dá chápat jako multiplikační tabulka operace bodového součinu vektorů délky $k$, kde se místo 0 píše $+1$ a místo 1 se píše $-1$.

Konstrukcí Hadamardových matic existuje celá řada. Přesto není dosud známo, zda takovou matici lze sestrojit pro každý řád dělitelný čtyřmi.

Z každé Hadamardovy matice $H$ řádu $n \geq 2$ se odvozuje binární kód $C(H)$ délky $n$ tak, že každému řádku $H$ se přiřadí dvě kódová slova: v jednom se hodnoty $+1, -1$ nahradí po řadě hodnotami $1, 0$, a v druhém se $+1, -1$ nahradí hodnotami $0, 1$. Protože počet shod i neshod dvou různých řádků je přesně $n/2$, je i Hammingova vzdálenost dvou kódových slov odvozených z dvou různých řádků přesně $n/2$ (kódová slova odvozená z téhož řádku mají Hammingovu vzdálenost maximální možnou, tj. $n$.) Kódům $C(H)$ se říká *Hadamardovy*. Mají parametry $(n, 2n, n/2)$.

**Tvrzení 7.2.** *Ať $H$ je Sylvestrova $H$-matice řádu $2^m$. Pak se $C(H)$ shoduje s Reed-Mullerovým kódem $\mathcal{R}(m, 1)$.*

*Důkaz.* Připomeňme, že pro booleovský polynom $a \in \mathbb{F}_2[x_1, \ldots, x_m]$ značí $v_a$ binární vektor délky $2^m$, který má v pozici $\sum \varepsilon_i 2^{m-i}$ hodnotu $a(\varepsilon_1, \ldots, \varepsilon_m)$.

Označme $s : \mathbb{F}_2[x_1, \ldots, x_m] \to \mathbb{F}_2[x_1, \ldots, x_{m+1}]$ zobrazení, které v každém polynomu nahradí proměnnou $x_i$ proměnnou $x_{i+1}$. Vyjádřit polynom $b \in \mathbb{F}_2[x_1, \ldots, x_{m+1}]$ ve tvaru $s(a)$ tudíž lze právě když $x_1$ nefiguruje v žádném monomu polynomu $b$. Pro dosazování platí vztah $s(a)(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m+1}) = a(\varepsilon_2, \ldots, \varepsilon_{m+1})$. Hodnota $v_{s(a)}$ v pozici $j = \sum_{i=1}^{m+1} \varepsilon_i 2^{m+1-i}$ je proto rovna hodnotě $v_a$ v pozici $j' = \sum_{i=1}^{m} \varepsilon_{i+1} 2^{m-i} = \sum_{i=2}^{m+1} \varepsilon_i 2^{m+1-i}$. Je-li $\varepsilon_1 = 0$, tak $j = j'$. Je-li $\varepsilon_1 = 1$, tak $j = 2^m + j'$. Pro $j < 2^m$ má tedy $v_{s(a)}$ v pozicích $j$ a $2^m + j$ hodnotu stejnou jako $v_a$ v pozici $j$, takže $v_{s(a)} = (v_a, v_a)$. Podobně $v_{x_1+s(a)} = (v_a, 1 + v_a)$.

Ať $H_2$ označuje Sylvestrovu $H$-matici řádu 2. Pro $m = 1$ tvrzení plyne z toho, že $\mathcal{R}(1, 1) = C(H_2) = \mathbb{F}_2^2$. Indukční přechod dostáváme z toho, že zdvojení $H \to (H \ H)$ souhlasí se zdvojením $v_a \to (v_a, v_a)$, zatímco $H \to (H \ -H)$ odpovídá $v_a \to (v_a, 1 + v_a)$. □

Ukážeme, že není možné konstruovat $(n, 2n, d)$ kódy tak, aby bylo $d > n/2$. Podobně ukážeme, že neexistují $(n, k, n/2)$ kódy, pro které by bylo $k > 2n$. Hadamardovy kódy jsou proto optimální pro volby parametrů $d \geq n/2$ a $k \geq 2n$.

**Tvrzení 7.3.** *Ať $C$ je $(n, k, d)$ kód takový, že $d > n/2$. Potom $k \leq 2d/(2d - n) \leq n + 1$.*

*Důkaz.* Představme si orientovaný graf s ohodnocenými hranami, které mohou být vícenásobné, jehož vrcholy jsou kódová slova $C$ a kde mezi $u, v \in C$, $u \neq v$, vede hrana ohodnocená dvojicí $(i, \alpha) \in \{1, \ldots, n\} \times \{0, 1\}$ právě když pro $u = (u_1, \ldots, u_n)$ a $v = (v_1, \ldots, v_n)$ máme $\alpha = u_i \neq v_i$. Celkový počet hran je alespoň $k(k - 1)d$, neboť mezi $u$ a $v$ vede právě $d(u, v) \geq d$ hran.

Označme $k(i, \alpha)$ počet $u \in C$, pro které je $\alpha = u_i$. V grafu se nachází právě $k(i, \alpha) \cdot (k - k(i, \alpha)) \leq k^2/4$ hran ohodnocených dvojicí $(i, \alpha)$. Proto je počet hran nejvýše $(2n)(k^2/4) = nk^2/2$. Dostáváme nerovnost $nk/2 \geq (k - 1)d$, ze které plyne $(2d - n)k \leq 2d$. Druhá nerovnost je patrná z $(n+1)(2d-n) - 2d = n(2d - n - 1) \geq 0$. □

Obdobný odhad lze získat i pro případ $q$-árních kódů, kde $q > 2$. Vychází se ze stejného grafu, úpravy jsou však o něco málo výpočtově náročnější. V binárním i obecném případě se mluví o *Plotkinově* odhadu.

**Tvrzení 7.4.** *Ať je $n$ sudé. Pro každý $(n, k, n/2)$ kód $C$ platí $k \leq 2n$.*

*Důkaz.* Pro $\alpha \in \{0, 1\}$ položme $C_\alpha = \{u \in C;\ u_1 = \alpha\}$ a označme $D_\alpha$ kód vzniklý propíchnutím $C_\alpha$ v pozici 1. Pak $D_\alpha$ (pokud $D_\alpha \neq \emptyset$) je $(n - 1, k_\alpha, d_\alpha)$ kód, kde $k_0 + k_1 = k$ a $d_\alpha \geq d$. Podle Tvrzení 7.3 máme $k_0 + k_1 \leq 2((n-1)+1) = 2n$. □

Kapitolu zakončíme tvrzením o existenci lineárních kódů, které je známo jako *Gilbert-Varšamovova nerovnost.*

**Tvrzení 7.5.** *Ať $n$, $k$ a $d$ jsou celá kladná čísla, $d \leq n$. Je-li $V_q(n, d-1) < q^{n-k+1}$, pak existuje $q$-ární $[n, k, d]$ kód.*

*Důkaz.* Předpokládejme, že jsme nalezli maximální lineární $q$-ární kód délky $n$ s minimální vzdáleností $d$. Označme $h$ jeho dimenzi. Zvolme celé $k > 0$ největší takové, že $V_q(n, d-1) < q^{n-k+1}$. Dokazované tvrzení je možno vyjádřit jako $h \geq k$. Nerovnost $h < k$ je možné zapsat jako $h + 1 \leq k$, a tedy jako $V_q(n, d-1) < q^{n-(h+1)+1} = q^{n-h}$. Pro důkaz sporem tedy stačí ověřit, že tato nerovnost vede ke sporu s maximalitou $C$.

Přepišme nejprve $V_q(n, d-1) < q^{n-h}$ jako $q^h V_q(n, d-1) < q^n$. Z nerovnosti plyne existence $u \in \mathbb{F}_2^n$, jež splňuje $d(u, x) \geq d$ pro každé $x \in C$. Položme $C' = \{\lambda u + x;\ \lambda \in \mathbb{F}_q \text{ a } x \in C\}$. Váha $\lambda u + x$ je pro $\lambda \neq 0$ stejná jako váha $u + \lambda^{-1} x$, a ta je rovna $d(u, -\lambda^{-1} x) \geq d$. Proto má $C'$ minimální váhu alespoň $d$. □

# 1 Asymptotické odhady

Cílem této kapitoly je vyložit nejpoužívanější asymptotické odhady omezující možné volby parametrů blokových kódů, z nichž některé platí pouze pro kódy lineární. Omezíme se pouze na kódy binární, důvody tohoto omezení budou však čistě technické. Pro $q$-ární kódy, kde $q \geq 3$, lze postupovat obdobně, příslušné vzorce ale bývají komplikovanější.

Prvním krokem je sestavení několika pomocných odhadů, které využívají tzv. entropickou funkci. Logaritmus o základu dvě budeme značit lg. Přirozený logaritmus se značí ln. Začneme tím, že připomeneme následující základní vlastnosti logaritmů.

**Lemma 1.1.** *Ať $x \in \mathbb{R}$, $0 < x < 1$. Pak*

*(i)* $\lg 1 = 0$, $\lg 2 = \ln e = 1$,

*(ii)* $\lg x = \ln x \lg e$ *a* $(\lg x)' = (\lg e)/x$,

*(iii)* $(x \lg x)' = \lg x + \lg e = \lg(ex)$,

*(iv)* $((1-x)\lg(1-x))' = -\lg(1-x) - \lg e = -\lg(e(1-x))$, *a*

*(v)* $\lim_{x\to 0} x \lg x = 0$.

□

*Entropickou funkci* $H$ definujeme pro $\alpha \in (0,1)$ vztahem

$$H(\alpha) = \alpha \lg \tfrac{1}{\alpha} + (1-\alpha) \lg \tfrac{1}{1-\alpha} = -\alpha \lg \alpha - (1-\alpha)\lg(1-\alpha).$$

Z Lemmatu 1.1 plyne, že $\lim_{x\to 0} H(x) = 0 = \lim_{x\to 1} H(x)$. Proto je možné $H$ spojitě dodefinovat v krajních bodech intervalu jako $H(0) = H(1) = 0$. Následující lemma uvádíme bez důkazu, neboť ten plyne z Lemmatu 1.1 přímočarým způsobem.

**Lemma 1.2.** *Entropická funkce $H$ je spojitě definovaná na intervalu $[0,1]$ a má tyto vlastnosti:*

*(i)* $H(\alpha) = H(1-\alpha)$ *pro každé* $\alpha \in [0,1]$, *takže $H$ je symetrická podle osy* $x = 1/2$.

*(ii) Pro každé* $\alpha \in (0,1)$ *platí* $H'(\alpha) = -\lg(\alpha) + \lg(1-\alpha)$, *takže $H$ je rostoucí na intervalu* $[0,1/2]$ *a klesající na intervalu* $[1/2,1]$.

*(iii)* $H'(1/2) = 0$ *a* $H(1/2) = 1$.

□

**Lemma 1.3.** *Ať $n \geq 1$ je celé. Pro každé reálné $r \in (0,n)$ platí*

$$2^{nH(\frac{r}{n})} = \frac{n^n}{r^r (n-r)^{(n-r)}}.$$

*Důkaz.* Z $1 - \frac{r}{n} = \frac{n-r}{n}$ plyne

$$nH(\tfrac{r}{n}) = n\tfrac{r}{n}\lg(\tfrac{n}{r}) + n\tfrac{n-r}{n}\lg(\tfrac{n}{n-r}) = \lg(\tfrac{n}{r})^r + \lg(\tfrac{n}{n-r})^{n-r} = \lg\frac{n^r n^{n-r}}{r^r(n-r)^{n-r}} = \lg\frac{n^n}{r^r(n-r)^{n-r}}.$$

□

Připomeňme, že $V(n,r)$ značí objem (tedy počet prvků) $n$-rozměrné koule s poloměrem $r$ počítané v Hammingově vzdálenosti.

**Lemma 1.4.** *Ať $n$ a $r$ jsou celá čísla, $0 \le r \le n/2$. Pak $V(n,r) = \sum_{i=0}^{r}\binom{n}{i} \le 2^{nH(r/n)}$. Je-li $r > 0$, platí tato nerovnost jako ostrá.*

*Důkaz.* Z $r \le n/2$ plyne $r/(n-r) \le 1$. Tudíž $1 \ge (\frac{r}{n-r})^{r-i}$, a tedy $r^i(n-r)^{n-i} \ge r^r(n-r)^{n-r}$ pro každé $i \ge 0$. Proto

$$n^n = (r + (n-r))^n = \sum_{i=0}^{n}\binom{n}{i}r^i(n-r)^{n-i} \ge \sum_{i=0}^{r}\binom{n}{i}r^n(n-r)^{n-r}.$$

Poslední nerovnost platí jako ostrá, pokud $r > 0$, neboť pak jsou vypouštěné členy nenulové. Zbytek plyne z Lemmatu 1.3. □

Uvedené důkazy pracují s poměrně velkoryse koncipovanými odhady. Pro důkazy asymptotických vztahů se takové odhady však ukazují jako dostačující. Pro práci s faktoriály proto také nebudeme využívat Stirlingovy formule

$$n! \approx \left(\frac{n}{e}\right)^n\sqrt{2\pi n},$$

ale spokojíme se s odhadem

$$\left(\frac{n}{e}\right)^n < n! \text{ pro } n \ge 0 \text{ a } n! < \left(\frac{n}{e}\right)^{n+1} \text{ pro } n \ge 50,$$

který je možné dokázat elementárně (což zde činit ovšem nebudeme).

**Lemma 1.5.** *Jsou-li $n$ a $k$ celá čísla, přičemž $k \ge 50$ a $n - k \ge 50$, tak platí*

$$\binom{n}{k} > 2^{nH(\frac{k}{n})}\frac{e^2}{k(n-k)}.$$

*Důkaz.* Z uvedeného odhadu výpočtu faktoriálu máme

$$\frac{n!}{k!(n-k)!} > \frac{n^n}{k^{k+1}(n-k)^{n-k+1}}\cdot\frac{e^{k+1}e^{n-k+1}}{e^n} = \frac{n^n}{k^k(n-k)^{n-k}}\cdot\frac{e^2}{k(n-k)}.$$

Zbytek plyne z Lemmatu 1.3. □

*Informační poměr* neboli *nosnost* $\alpha(C)$ binárního $(n, k, d)$ kódu $C$ se definuje jako $(\lg k)/n$. Pro $[n, k, d]$ kód $C$ je tedy $\alpha(C) = k/n$.

*Relativní vzdáleností* se rozumí poměr $d/n$.

Ať $\mathcal{C}$ je nějaká třída sestávající se z nekonečně mnoha různých binárních kódů. Řekneme o ní, že je *asymptoticky dobrá,* jestliže existují konstanty $\alpha_0$ a $\delta_0$ takové, že

$$\alpha(C) > \alpha_0 > 0 \text{ a } \delta(C) > \delta_0 > 0 \text{ pro všechna } C \in \mathcal{C}.$$

Mnohé standardně studované třídy binárních kódů asymptoticky dobré nesou. U jiných odpověď není známa. Asymptoticky dobré třídy binárních kódů však existují a jsou známy. Jejich konstrukce bývá založena na iterativních postupech, kterým jsme se zde nevěnovali.

Pro $n \geq d \geq 1$ definujme $A(n, d)$ jako maximum ze všech hodnot $\lg k$ takových, že existuje $(n, k, d)$ kód.

Poměr $A(n, d)/n$ tedy udává nejvyšší možnou nosnost při zadané délce a minimální vzdálenosti. Limitním přechodem pak dostáváme asymptotickou nosnost při zadané relativní vzdálenosti, a to vztahem

$$\alpha(\delta) = \limsup_{n\to\infty} \frac{A(n, \lceil \delta n \rceil)}{n}.$$

**Lemma 1.6.** *Ať $1 \leq d \leq n/2$. Potom $A(n, d) \geq n(1 - H(\frac{d-1}{n}))$, přičemž pro $d > 1$ platí ostrá nerovnost.*

*Důkaz.* Případ $d = 1$ vede na totální kód a je zřejmý. Proto lze předpokládat $d > 1$. Podle Lemmatu 1.4 je $\lg V(n, d-1) < nH(\delta)$, kde $\delta = (d-1)/n$. Z Tvrzení **??** tedy víme, že $[n, k, d]$ kód existuje, jestliže $nH(\delta) \leq n - k + 1$. Podmínku $k \leq n(1 - H(\delta)) + 1$ splňuje alespoň jedno celé $k \geq n(1 - H(\delta))$, a proto $A(n, d) \geq k \geq n(1 - H(\delta))$. □

Můžeme tudíž vyslovit tzv. *asymptotický Gilbert-Varšamovův odhad:*

**Tvrzení 1.7.** *Ať $0 < \delta \leq 1/2$. Pak $\alpha(\delta) \geq 1 - H(\delta)$.*

*Důkaz.* Podle Lemmatu 1.6 pro dostatečně velké $n$

$$\frac{A(n, \lceil \delta n \rceil)}{n} > 1 - H\left(\frac{\lceil \delta n \rceil - 1}{n}\right),$$

takže pro dokončení důkazu stačí ověřit nerovnost $\frac{\lceil \delta n \rceil - 1}{n} \leq \delta$, neboť funkce $H$ je na intervalu $[0, 1/2]$ podle Lemmatu 1.2 rostoucí. Platnost nerovnosti vyplývá z toho, že ji lze vyjádřit jako $\lceil \delta n \rceil \leq \delta n + 1$. □

Protipólem k předchozímu odhadu je tzv. *asymptotický Hammingův odhad:*

**Tvrzení 1.8.** *Pro každé $\delta$, $0 < \delta < 1$, platí $\alpha(\delta) \leq 1 - H(\delta/2)$.*

*Důkaz.* Pro každé $n \geq 8$ položme $\mu(n) = \max\{|\lg e^2 - \lg r - \lg(n-r)|;\ 0 < r < n\}$. Zjevně $\mu(n) \leq 2\lg n$, takže $\lim_{n\to\infty} \mu(n)/n = 0$. Členy asymptotických odhadů, které limitně míří k nule, je zvykem označovat $o(1)$. Podle lemmat 1.4 a 1.5 máme $V(n,r) > \binom{n}{r} > 2^{nH(r/n)} e^2 r^{-1}(n-r)^{-1}$ pro všechna celá $r$ a $n$, která splňují $r \geq 50$ a $n \geq r + 50$. Proto v takovém případě $\lg V(n,r) > \lg \binom{n}{r} > nH(\frac{r}{n}) + \lg e^2 - \lg r - \lg(n-r)$, takže $\frac{\lg V(n,r)}{n} > H(\frac{r}{n}) + o(1)$.

Z Hammingova odhadu víme, že kódy s minimální vzdáleností $d \geq 2r+1$ mají méně než $2^n/V(n,r)$ prvků. Z $[\frac{\delta n-1}{2}] \leq \frac{\delta n-1}{2}$ plyne $2[\frac{\delta n-1}{2}] + 1 \leq \lceil \delta n \rceil$, takže

$$\frac{A(n, \lceil \delta n \rceil)}{n} \leq \frac{1}{n} \lg \left( \frac{2^n}{V(n, [\frac{\delta n-1}{2}])} \right) = 1 - \frac{\lg V(n, [\frac{\delta n-1}{2}])}{n}$$
$$< 1 - H\left( \frac{[\frac{\delta n-1}{2}]}{n} \right) - o(1).$$

Zbytek plyne z limitního přechodu, Lemmatu 1.2 a nerovností

$$\frac{1}{2} > \frac{1}{n}\left[\frac{\delta n - 1}{2}\right] > \frac{\delta n - 1}{2n} = \frac{\delta}{2} - \frac{3}{2n}.$$

□

# 1 Teorie informace

Mějme nějakou abecedu $\mathbb{A}$ nad konečným počtem symbolů $a_1, \ldots, a_n$. Při používání $\mathbb{A}$ ať se každé $a_i \in \mathbb{A}$ vyskytuje s frekvencí $p_{a_i} = p_i$. Je tedy $\sum p_i = 1$.

Předpokládejme, že bychom chtěli zavést jakýsi binární těsnopis, který by komunikaci pomocí symbolů abecedy $\mathbb{A}$ co nejvíce komprimoval. Jde o jednoduchou myšlenku, kterou ilustrujeme na příkladě, ve kterém frekvence $p_i$ upravíme tak, aby souvislost s binárními zápisem co nejlépe vynikla.

Za symboly abecedy $\mathbb{A}$ budeme považovat smutně realistické frekvence povelů psovi Hafíkovi uvedené v následující tabulce.

| Symbol | Povel | frekvence | binárně |
|---|---|---|---|
| $a_1$ | SEDNI | 1/4 | 00 |
| $a_2$ | LEHNI | 1/4 | 01 |
| $a_3$ | DEJ POKOJ | 1/4 | 10 |
| $a_4$ | DO BOUDY | 1/8 | 110 |
| $a_5$ | APORT | 1/16 | 1110 |
| $a_6$ | HLEDEJ | 1/32 | 11110 |
| $a_7$ | PAC | 1/64 | 111110 |
| $a_8$ | VEM SI HO | 1/64 | 111111 |

Nejméně frekventované povely jsou nejpřekvapivější, a proto lze říci, že nesou nejvíce informace. To je vyjádřeno i tím, že při snaze o co nejúspornější záznam komunikace je jim věnováno nejvíce bitů. Jejich počet budeme považovat za (binární) *informační obsah* povelu. V našem případě to jsou po řadě čísla 2, 2, 2, 3, 4, 5, 6, 6. Obecně nemusíme dostat celé číslo – hodnotou informačního obsahu $I(a_i)$ symbolu $a_i$ definujeme jako $\lg(1/p_i)$, kde lg znamená logaritmus při základu dva.

Podobný postup jako ten, který jsme naznačili výše, se používá při některých typech komprimace textu. Podle frekvence výskytu slov či frází se vybuduje binární strom, na jehož koncových uzlech jsou umístěna slova či fráze tak, aby součet frekvencí koncových uzlů levé části byl zhruba stejný jako součet frekvencí koncových uzlů v pravé části (oba součty tedy aproximují hodnotu 1/2). Rekurzivně se pak pokračuje i při dalších větveních. Takto vytvořeným kódům se říká *Huffmanovy*.

Hodnoty $p_i$ jsme volili jako pravděpodobnosti výskytu symbolu $a_i$, tedy $p_i = \Pr(a_i)$. Pro další úvahy učiníme zjednodušující předpoklad, že sled symbolů abecedy $\mathbb{A}$ není kontextově závislý. To je samozřejmě předpoklad, který ve většině aplikací splněn nebude, nicméně bez něj by se následující úvahy nesmírně komplikovaly. Tyto úvahy přitom vedou k silné teorii, která se zpětně využívá i tak, že se pořadí vysílaných symbolů na určitém dostatečně velkém úseku permutuje, takže jejich pořadí se skutečně pak jako kontextově nezávislé jeví.

Jinými slovy, budeme předpokládat, že pro slovo $a_{i_1} \dots a_{i_k} \in \mathbb{A}^*$ máme

$$\Pr(a_{i_1} \dots a_{i_k}) = \Pr(a_{i_1}) \dots \Pr(a_{i_k}) = p_{i_1} \dots p_{i_k} = \prod p_{i_j}.$$

Z kontextové nezávislosti vyplývá, že z předchozího toku symbolů nelze odvodit obsah následující. Proto se míra informace obsažená ve dvou za sebou následujících úsecích rovná součtu informačního obsahů jednotlivých úseků. Dostáváme

$$I(a_{i_1} \dots a_{i_k}) = I(a_{i_1}) + \dots + I(a_{i_k}) = \sum \lg \frac{1}{p_{i_j}} = \lg \frac{1}{\prod p_{i_j}}.$$

Slovo „entropie“ je používáno v mnoha různých významech. Obecně znamená absenci nějakého řádu, který by umožnil rozlišovat mezi jednotlivými součástmi systému. Etymologicky „entropický“ znamená „dovnitř obrácený“, což vzniklo jako snaha popsat v termodynamice tu část energie systému, kterou nelze použít pro vykonání práce. V naší situaci se absencí řádu možná poněkud překvapivě míní malá odlišnost frekvencí symbolů. Jde o pojem definovaný, kde vést úvahy o vhodnosti volby slova má jen omezený význam. Poznamenejme však, že jazyk, ve kterém by všechna slova měla stejnou frekvenci, by byl pro zvládnutí skutečně velmi obtížný.

Stanovení frekvencí $p_i$ vyžaduje nějaký tok dat symbolů abecedy $\mathbb{A}$. Mluvíme o *informačním zdroji* $\mathcal{A}$ – formálně ho lze například popsat jako nekonečnou posloupnost symbolů abecedy $\mathbb{A}$, přičemž frekvence $p_i$ vyjadřují limitní hodnoty počítané z konečných počátečních úseků. *Entropií* informačního zdroje $\mathcal{A}$ se pak rozumí průměrná informační hodnota symbolů abecedy $\mathbb{A}$. Používáme označení $\mathcal{H}(\mathcal{A})$, takže platí

$$\mathcal{H}(\mathcal{A}) = \sum p_i I(a_i) = \sum p_i \lg(\frac{1}{p_i}).$$

Pro náš úvodní příklad vychází entropie $3 \cdot 2/4 + 3/8 + 4/16 + 5/32 + 2 \cdot 6/64 = 79/32$. Pokud by všech osm povelů mělo stejnou frekvenci, dostali bychom entropii vyšší, a to $8 \cdot 3/8 = 3$. Prvá souvislost s entropickou funkcí $H$ se ukazuje v případě, kdy informační zdroj $\mathcal{A}$ je binární (má tedy pouze dva symboly). Pokud $p = p_1$, tak $p_2 = 1 - p$ a $\mathcal{H}(\mathcal{A}) = p \lg p^{-1} + (1-p) \lg(1-p)^{-1} = H(p)$. Tato souvislost však nebude tou hlavní, k té dospějeme teprve úvahami o spolehlivosti kanálu.

Entropii informačního zdroje můžeme neformálně chápat jako průměrnou sdělnost znaku abecedy $\mathbb{A}$, což například znamená, že při převodu do optimalizovaného binárního zápisu je na záznam zprávy délky $k$ potřeba $k \cdot \mathcal{H}(\mathcal{A})$ bitů (ve skutečnosti to bude o něco více díky necelým hodnotám). Na informační obsah symbolu se též můžeme dívat jako na míru překvapení, že se ve zprávě symbol objevil (tak jako pes Hafík bude spíše překvapen, že si má někoho vzít než že má dát pokoj). Entropii tedy můžeme také chápat jako průměrnou míru překvapení.

Předpokládejme nyní, že informační zdroj $\mathcal{A}$ prochází nějakou transformací (obvykle se mluví o průchodu kanálem), po jejímž provedení se mění na informační zdroj $\mathcal{B}$. Symboly $\mathcal{A}$ nechť se vyskytují s frekvencemi $p_i$ a synboly $\mathcal{B}$ s

frekvencemi $q_j$. Předpokládáme, že kanál mění symbol na symbol, a to tak, že $i$-tý vstupní symbol $a_i$ přejde na $j$-tý výstupní symbol $b_j$ s pravděpodobností $p_{ij}$. Počet vstupních symbolů buď roven $n$ a počet výstupních symbolů ať je $m$. Z pravděpodobností $p_{ij}$ vytvořme matici $P = (p_{ij})$ rozměrů $n \times m$. Vidíme, že platí

$$(p_1, \ldots, p_n)P = (q_1, \ldots, q_m).$$

Formálně vzato můžeme transformaci $\mathcal{A} \to \mathcal{B}$ považovat za reversibilní, tedy uvažovat opačný průchod kanálem. Pravděpodobnost přechodu $b_j$ na $a_i$ označíme $q_{ji}$. Hodnoty $p_{ij}$ a $q_{ji}$ jsou vlastně podmíněné pravděpodobnosti $\Pr(b_j|a_i)$ a $\Pr(a_i|b_j)$. Ze vztahu

$$\Pr(a_i)\ \Pr(b_j|a_i) = \Pr(a_i, b_j) = \Pr(b_j)\ \Pr(a_i|b_j)$$
$$\text{vyplývá}\ \ p_i p_{ij} = q_j q_{ji},\ \text{takže}\ \ q_{ji} = \frac{p_i}{q_j} p_{ij}.$$

Uvažme nyní informační obsah zjištění při přijetí symbolu $b_j$, že byl vyslán symbol $a_i$. Frekvence jsou v takto zúženém případě rovny $q_{j1}, \ldots, q_{jn}$, takže relativní informační obsah $I(a_i|b_j)$ je roven $\lg(1/q_{ji})$. Můžeme ho považovat za míru překvapení, když se dozvíme, že byl vyslán symbol $a_i$. Pokud by obě abecedy splývaly a informační kanál byl pouze identickým opakováním, tak bude $q_{jj} = 1$ a $q_{ji} = 0$ pro $i \neq j$. V takovém případě je překvapení při přijetí shodného symbolu nulové, zatímco při přijetí odlišného symbolu (k čemuž nemůže dojít) by bylo překvapení nekonečně velké. Pokud známe pouze informační zdroj $\mathcal{B}$, je pro nás informace odpovídající zjištění vyslaného symbolu $a_i$ nedostupná. Vážený průměr $\mathcal{H}(\mathcal{A}|b_j)$ informačních obsahů $I(a_i|b_j)$ je tedy roven průměrnému ztracenému informačnímu obsahu při příjmu symbolu $b_j$, a vážený průměr $\mathcal{H}(\mathcal{A}|\mathcal{B})$ přes všechna $b_j$ udává průměrnou ztrátu informačního obsahu na jeden symbol. Máme

$$\mathcal{H}(\mathcal{A}|b_j) = \sum_i q_{ji} \lg \frac{1}{q_{ji}} \quad \text{a} \quad \mathcal{H}(\mathcal{A}|\mathcal{B}) = \sum_j q_j \mathcal{H}(\mathcal{A}|b_j) = \sum_j q_j \sum_i q_{ji} \lg \frac{1}{q_{ji}},$$

Průměrný informační obsah jednoho symbolu z $\mathcal{A}$ je rovna $\mathcal{H}(\mathcal{A})$, takže

$$I(\mathcal{A}, \mathcal{B}) = \mathcal{H}(\mathcal{A}) - \mathcal{H}(\mathcal{A}|\mathcal{B})$$

udává průměrný informační obsah přijatého symbolu. Je ovšem otázka, zda tento obsah lze skutečně efektivně zpřístupnit. Ukážeme na jednom konkrétním případu kanálu, že pomocí samoopravných kódů to možné je.

Typem kanálu, který budeme uvažovat, je nejjednodušší netriviální případ, a to takzvaný *binární symetrický kanál*, zkráceně BSC, ve kterém se vysílají i přijímají dva symboly, přičemž k chybě dochází s pravděpodobností $p = p_{12} = p_{21}$. Předpokládáme, že oba vysílané symboly jsou stejně frekventované, tedy $p_1 = p_2 = 1/2$. Máme $p_{11} = p_{22} = 1 - p$ a

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix},$$

takže $q_1 = q_2 = 1/2$, $q_{12} = q_{21} = p$ a $q_{11} = q_{22} = 1 - p$.

Vidíme, že $\mathcal{H}(\mathcal{A}|\mathcal{B}) = 2(1/2)(p\lg(1/p) + (1-p)\lg(1/(1-p))) = H(p)$. Dále $\mathcal{H}(\mathcal{A}) = 2(1/2)H(1/2) = 1$, takže $I(\mathcal{A},\mathcal{B}) = 1 - H(p)$. Hodnota $C(p) = 1 - H(p)$ se nazývá *kapacita kanálu*. Pravděpodobnosti $p$ se říká *chybovost* kanálu.

Nyní uvedeme (hlavní) Shannonovu větu, zvanou též Základní věta teorie informací. Připomeňme, že informačním poměrem (nosností) binárního kódu $C$ délky $n$, který má $k$ kódových slov, rozumíme hodnotu $\alpha(C) = (\lg k)/n$. Dekódováním metodou nejbližšího slova rozumíme algoritmus, ve kterém přijatému slovu $v$ přiřadíme kódové slovo $u$, které má nejmenší Hammingovu vzdálenost $d(u,v)$, a to jen tehdy, pokud takové kódové slovo $u$ existuje.

**Věta 1.1.** *Ať je dán BSC kanál s chybovostí $p$, kde $0 < p < 1/2$. Pak pro všechna $\varepsilon > 0$ a $\delta > 0$ existuje $n_0 > 1$, že pro každé $n > n_0$ existuje binární kód $C$ délky $n$ takový, že $1-H(p) > \alpha(C) \geq 1-H(p)-\varepsilon$, ve kterém dekódování metodou nejbližšího kódového slova selhává s pravděpodobností menší než $\delta$.*

*Nástin důkazu.* Podrobný a přesný důkaz uvedeme v závěru kapitoly. Zde je cílem seznámení s jeho hlavními myšlenkami. Přitom se nebudeme vyjadřovat vždy formálně zcela přesně. Ukážeme, že našemu požadavku vyhoví každý kód $C$, který je vybrán dostatečně náhodně a který má pro nějaké $R < 1 - H(p)$ přesně $2^{nR}$ slov. Je tedy $R = \alpha(C)$. Přitom $R$ volíme při zadaném $\varepsilon$ tak, aby existovalo nějaké $\gamma > 0$, že $1 - H(p) - \varepsilon \leq R \leq 1 - H(p) - \gamma$. Náhodnost $C$ znamená, že kódových slov v kouli o poloměru $j$ je relativně stejně jako v celém kódu. Čili předpokládáme, že

$$|\{u \in C;\ d(u,v) \leq j\}| = \frac{2^{nR}}{2^n} \sum_{i \leq j} \binom{n}{i},$$

pro všechna $j$, která jsou dostatečně malá. Na pravé straně rovnosti nemusí být samozřejmě celé číslo; ve skutečnosti nejde o rovnost, ale o průměrný počet kódových slov. Náhodnost $C$ zaručuje, že opakované náhodné volby koule o poloměru $j$ dávají tento průměrný počet.

Pro dostatečně velká $n$ lze předpokládat, že chyb při přenosu je asi $pn$. Přesněji to vymezuje zákon velkých čísel, ze kterého, jak níže uvidíme, vyplyne, že přijaté slovo $v$ se od vyslaného $u$ liší natolik málo, že lze předpokládat, že $d(u,v)$ je v blízkosti $pn$. Hodnotu blízkou $pn$ budeme volit jako poloměr koule, kterou použijeme pro dekódování. Problém může nastat v tom, že by vedle $u$ existovalo ještě nějaké $u' \in C$, které by také leželo ve vzdálenosti málo odlišné od $pn$, případně ve vzdálenosti menší. Ukážeme, že z pravděpodobnostního hlediska tomu tak není. Vtip je v tom, že existenci $u$ máme zaručenou přenosem, ale existence $u'$ už je záležitostí náhodnou, na kterou lze použít předpoklad o náhodném charakteru kódu $C$. V kouli o poloměru $pn$ najdeme průměrně kódových slov

$$\frac{2^{nR}}{2^n} \sum_{i \leq pn} \binom{n}{i} \leq 2^{nH(p)} \frac{2^{nR}}{2^n} = 2^{-n(1-H(p)-R)} \leq 2^{-n\gamma}.$$

Uvedená nerovnost plyne z Lemmatu **??**. Vidíme, že s rostoucím $n$ se pravděpodobnost výskytu jakéhokoliv slova v kouli poloměru $pn$ blíží nule. Proto se blíží nule i pravděpodobnost existence kódového slova $u' \neq u$. □

Jako fakt nyní uvedeme takzvaný Slabý zákon velkých čísel. Ten se dokazuje v teorii pravděpodobnosti. Je založen na pradávné zkušenosti z oblasti hazardních her, že při dostatečném počtu opakování hodů se dosahuje stejného stabilního průměrného chování. Dá se s jistou nadsázkou také říci, že teorie pravděpodobnosti byla vybudována právě tak, aby v ní tento zákon platil. Proto není nutné na jeho důkaz formálně odkazovat.

**Věta 1.2.** *Ať $x_1, x_2, \ldots$ je posloupnost, jejíž členy nabývají náhodně reálných hodnot $a_1, a_2, \ldots, a_m$, a to s pravděpodobnostmi $p_1, \ldots, p_m$. Položme $\mu = \sum p_j a_j$. Pak pro každé $\varepsilon > 0$ je*

$$\lim_{n\to\infty} \Pr\left(\left|\frac{1}{n}\sum_{i=1}^{n} x_i - \mu\right| > \varepsilon\right) = 0.$$

Poznamenejme, že členům $x_i$ (jednotlivým „tahům“) se v teorii pravděpodobnosti říká náhodné proměnné.

Při přenosu pomocí BSC s chybovostí $p$ odpovídají proměnné $x_i$ úspěšnosti přenosu $i$-tého symbolu. Nedošlo-li k chybě, položíme $x_i = 0$, naopak při chybě bude $x_i = 1$. Je-li $u = u_1 \ldots u_n$ vyslané slovo a $v = v_1 \ldots v_n$ slovo přijaté, tak $\sum x_i = d(u, v)$. Podle Věty 1.2 je

$$\lim_{n\to\infty} \Pr\left(|d(u, v) - pn| > n\varepsilon\right) = 0.$$

Podmínku $|d(u, v) - pn| \leq n\varepsilon$ můžeme také zapsat jako $v \in M(u, \varepsilon)$, kde $M(u, \varepsilon) = \{x \in \mathbb{F}_2^n;\ n(p - \varepsilon) \leq d(u, x) \leq n(p + \varepsilon)\}$. Zákon velkých čísel tedy říká, že pro libovolné $\varepsilon > 0$ lze pro stanovené $\delta > 0$ najít $n_0$ tak, že pro každé $n > n_0$ je $v \in M(u, \varepsilon)$ s pravděpodobností větší než $1 - \delta$. Tato skutečnost doplňuje nástin důkazu Věty 1.1 a níže ji ještě několikrát využijeme.

Pravděpodobnost, že $u = u_1 \ldots u_n$ je přeneseno jako $v = v_1 \ldots v_n$ lze také vyjádřit jako $p^d(1 - p)^{n-d}$, kde $d = d(u, v)$. Předokládáme $0 < p < 1/2$, takže tato pravděpodobnost s rostoucí vzdáleností od $u$ klesá. Prvek $v \in M(u, \varepsilon)$ má nejmenší možnou vzdálenost od $u$ rovnou $n(p - \varepsilon)$, a proto pravděpodobnost transformace $u$ na $v \in M(u, \varepsilon)$ je shora omezena hodnotou

$$p^{n(p-\varepsilon)}(1 - p)^{n(1-p+\varepsilon)} = p^{np}(1 - p)^{n(1-p)} \left(\frac{1 - p}{p}\right)^{n\varepsilon}.$$

Protože $p^{np}(1-p)^{n(1-p)} = 2^{np \lg p} 2^{n(1-p)\lg(1-p)} = 2^{-nH(p)}$, tak můžeme vyslovit

**Lemma 1.3.** *Při přenosu BSC kanálem s chybovostí $0 < p < 1/2$ uvažme binární slova $u$ a $v$ délky $n \geq 1$. Ať $0 < \varepsilon < 1$. Je-li $u$ slovo vyslané a $v \in M(u, \varepsilon)$, tak pravděpodobnost toho, že $v$ bude slovo přijaté, je shora omezena hodnotou $2^{-nH(p)}((1 - p)/p)^{n\varepsilon}$.*

Kapacita kanálu je ostrým předělem pro nosnost (informační poměr) $\alpha(C)$ kódu $C$. Podle Shannonovy věty 1.1 lze konstruoovat libovolně spolehlivé kódy pokud připustíme, aby nosnost byla menší než kapacita kanálu. Přitom není potřeba vymýšlet nějaké chytré strategie dekódování – vystačíme s dekódováním

pomocí nejbližšího slova. Smyslem obrácené Shannonovy věty 1.5 bude naopak dokázat, že při použití libovolné metody dekódování nemůžeme dosáhnout uspokojivé spolehlivosti přenosu, pokud nosnost kódu převýší kapacitu kanálu. Tato skutečnost odpovídá pozorováním o ztrátě informace, ukážeme navíc, že pro dostatečně velká $n$ je kvalita přenosu „libovolně špatná“.

Spolehlivost dekódování se vždy vztahuje k nějakému algoritmu, který z přijatého slova vytváří slovo kódové. Tento algoritmus musí být efektivně dostupný, pro naše účely však stačí, abychom si uvědomili, že musí realizovat nějaké zobrazení $D : \mathbb{F}_2^n \to C$, kde $n$ je délka binárního kódu $C$. *Spolehlivostí dekódování* $D$ se rozumí průměrná pravděpodobnost, že $D(v) = u$, kde $(u, v)$ probíhá všechny možné dvojice odpovídající vyslanému a přijatému slovu. Je to ovšem průměr vážený, kde váha dvojice $(u, v)$ je dána pravděpodobností, že $v$ bude slovo přijaté. Tato pravděpodobnost závisí na chybovosti kanálu $p$ (a už jsme se jí výše zabývali). *Spolehlivostí kódu* $C$ pak budeme rozumět maximální spolehlivost počítanou přes všechna zobrazení $D : \mathbb{F}_2^n \to C$. Zdůrazněme, že spolehlivost se počítá vždy relativně vůči dané chybovosti.

Při důkazu Věty 1.5 se bude hodit následující elementární pozorování.

**Lemma 1.4.** *Jestliže jev $A$ nastává s pravděpodobností $a$ a jev $B$ s pravděpodobností $b$, tak jev $A \cap B$ nastává s pravděpodobností alespoň $a + b - 1$.*

*Důkaz.* Označme $x$ pravděpodobnost jevu $A \cap B$. Potom $a - x$ je pravděpodobnost jevu $A \setminus B$. Ta je $\leq$ pravděpodobnost doplňkového jevu $B'$, takže $a - x \leq 1 - b$. □

**Věta 1.5.** *Ať $\gamma$ a $p$ jsou reálná čísla, která splňují $0 < \gamma < 1$ a $0 < p < 1/2$. Uvažujme BSC chybovosti $p$. Pro každé $R > 1 - H(p)$ existuje celé číslo $n_0$, že každý binární kód délky $n \geq n_0$, který splňuje $\alpha(C) \geq R$, má spolehlivost $\leq \gamma$.*

*Důkaz.* Budeme postupovat sporem, tedy budeme předpokládat, že existuje $1 > \gamma > 0$ takové, že pro libovolně velká $n$ lze nalézt kód $C$ a zobrazení $D : \mathbb{F}_2^n \to C$ tak, aby průměrná (vážená) pravděpodobnost toho, že pro dvojici $(u, v)$ vyslaného a přijatého slova platí $D(v) = u$, byla $\geq \gamma$.

Podle Zákona velkých čísel pro každé $\varepsilon > 0$ platí, že pro dostatečně velká $n$ je $v \in M(u, \varepsilon)$ s pravděpodobností $\geq 1 - \gamma/2$. Podle Lemmatu 1.4 je pravděpodobnost souběhu jevů $D(v) = u$ a $v \in M(u, \varepsilon)$ alespoň $\gamma + (1 - \gamma/2) - 1 = \gamma/2$. Tedy

$$\Pr\left(v \in D^{-1}(u) \cap M(u, \varepsilon)\right) \geq \gamma/2.$$

Podle Lemmatu 1.3 je uvedená pravděpodobnost pro jedno konkrétní $u \in C$ shora omezena hodnotou

$$2^{-nH(p)} \left(\frac{1-p}{p}\right)^{n\varepsilon} \left|D^{-1}(u) \cap M(u, \varepsilon)\right|.$$

Součet těchto hodnot počítaný přes všechna $u \in C$ je tedy horním odhadem $\Pr\left(v \in D^{-1}(u) \cap M(u, \varepsilon)\right)$. Označme $k$ počet kódových slov kódu $C$ a

všimněme si, že množiny $D^{-1}(u)$, kde $u$ probíhá $C$, jsou po dvou disjunktní. Dokázali jsme, že

$$2^n \geq \sum_{u \in C} \left| D^{-1}(u) \cap M(u, \varepsilon) \right| \geq \frac{k\gamma}{2} 2^{nH(p)} \left( \frac{p}{1-p} \right)^{n\varepsilon}.$$

Úvahu dovedeme ke sporu tím, že ukážeme, že při dostatečně malém $\varepsilon > 0$ a při dostatečně velkém $n$ je pravá strana větší než $2^n$. Podle předpokladu o $\alpha(C)$ je $\lg k \geq Rn$ a $R > 1 - H(p)$. Logaritmus pravé strany je tedy roven

$$Rn + nH(p) + \lg \frac{\gamma}{2} + n\varepsilon \lg \frac{p}{1-p} = n \left( R + H(p) + \varepsilon \lg \frac{p}{1-p} + \frac{1}{n} \lg \frac{\gamma}{2} \right).$$

Platí $R + H(p) > 1$. Hodnoty $\lg(p/(1-p))$ a $\lg(\gamma/2)$ jsou záporné, ale konstantní. Vhodnou volbou $\varepsilon$ a $n$ lze proto učinit odpovídající členy natolik malé, aby celý výraz měl hodnotu přesahující $n$. □

Zbývá uvést úplný důkaz Shannonovy věty.

*Důkaz Věty 1.1.* Budeme pracovat s hodnotou $\rho = n(p + \eta)$, kde $\eta > 0$ nebude záviset na $n$, ale pouze na $\varepsilon > 0$. Jeho volbu upřesníme až v závěrečné části důkazu..

Hledáme binární kód $C$ délky $n$, který má $k$ kódových slov tak, aby bylo $(\lg k)/n < 1 - H(p)$ a aby metoda volby nejbližšího kódového slova chybovala s libovolně malou předem určenou pravděpodobností $\delta > 0$.

Vyslané kódové slovo budeme opět značit $u$, zatímco $v$ bude označovat slovo přijaté. Prostor jevů, k němuž se vztahují námi zkoumané a odhadované pravděpodobnosti, je tedy prostor všech možných dvojic $(u, v)$. Případ, kdy se $v$ octne mimo v Hammingově vzdálenosti větší než $\rho$, budeme považovat bez bližšího zkoumání za případ neúspěšného dekódování. Pravděpodobnost nesprávného dekódování lze tedy shora odhadnout jako

$$\Pr\left(d(u, v) > \rho\right) + \Pr\left((C \setminus \{u\}) \cap S(v, \rho) \neq \emptyset\right).$$

Druhou z uvedených pravděpodobností převedeme na zkoumání, zda dané $u' \in C$ se nachází v blízkosti nějakého přijatého slova $v$ a je přitom různé od $u$. Probíhá-li $u'$ celý kód $C$, můžeme součet všech takových pravděpodobností s jistou zkratkovitostí zapsat jako

$$\sum_{u' \neq u} \Pr\left(d(u', v) \leq \rho\right).$$

Touto sumou můžeme nahradit pravý sčítanec ve výše uvedeném odhadu. Při nahrazování jde o horní odhad, neboť v některé kouli se mohou vyskytovat dvě různá $u'$.

Již jsme dokázali, že ze Zákona velkých čísel 1.2, plyne, že $v \in M(u, \eta)$ pro dostatečně velká $n$ s libovolně velkou pravděpodobností. Pro každé uvažované $\eta$ lze tedy najít $n_0$ tak, že pro $n > n_0$ je $\Pr\left(d(u, v) > \rho\right) < \delta/2$.

Abychom vhodně vyjádřili $\sum_{u' \neq u} \Pr\left(d(u', v) \leq \rho\right)$, rozšíříme jevový prostor na trojice $(u, u', v)$, kde $u, u' \in C$, $u$ je vyslané slovo a $v$ je přijaté slovo. Příznivým jevem je ten, kdy $u' \neq u$ a $d(u', v) \leq \rho$. Hledaná pravděpodobnost je pak rovna $k$-násobku pravděpodobnosti příznivého jevu (připomeňme, že $k$ udává velikost kódu $C$).

Uvažme chybový vektor $e = v - u$ a položme $w = u' - u$. Máme $d(u', v) \leq \rho$ právě když $d(w, e) \leq \rho$. Místo jevového prostoru daného trojicemi $(u, u', v)$ můžeme tedy vyšetřovat jevový prostor trojic $(u, w, e)$, kde $u \in C$, $w \in u + C$, a příznivým jevem je $w \neq 0$ a $d(w, e) \leq \rho$. Váha jevového podprostoru s pevným $e$ je dána pravděpodobností chyby přesně v nenulových pozicích $e$, čili je rovna $p^{|e|}(1-p)^{n-|e|}$. Počet příznivých jevů je roven hodnotě

$$\mu_C(e, \rho) = \left|\left\{(u, u') \in C \times C;\ u \neq u' \text{ a } |(u' - u) - e| \leq \rho\right\}\right|,$$

takže pravděpodobnost příznivého jevu pro dané $e$ je rovna $\mu_C(e, \rho)/k^2$. Pro důkaz potřebujeme vyjádření $k$-násobku souhrnné pravděpodobnosti příznivého jevu, a tou, jak vidíme, je

$$\frac{1}{k} \sum_{e \in \mathbb{F}_2^n} p^{|e|}(1-p)^{n-|e|} \mu_C(e, \rho).$$

Pro dokončení důkazu potřebujeme ověřit, že pro každé dostečně velké $n$ existuje binární kód $C$ s dostatečně velkou nosností $\alpha(C)$, pro který je uvedená hodnota menší než $\delta/2$. Vtip důkazu spočívá v tom, že se kód $C$ nekonstruuje explicitně, ale celá hodnota se počítá tak, jako by $C = \{u_1, \ldots, u_k\}$ bylo proměnným parametrem. Pokud průměr přes všechna $C$ při vhodně zvoleném $k$ vyjde $< \delta/2$, musí samozřejmě nějaké hledané $C$ existovat (a je jich dokonce naprostá většina).

Pro účely výpočtu je výhodné kód $C$ neuvažovat jako $k$-bodovou množinu, ale jako uspořádanou posloupnost $k$ různých prvků. Všech kódů délky $k$ je $2^n!/(2^n - k)!$. Pokud pro nějaké pevné vektory $u \neq u'$ délky $n$, požadujeme, aby platilo $u_i = u$ a $u_j = u'$, kde $1 \leq i < j \leq k$, tak je počet takových kódů roven zlomku, kde v čitateli je počet všech kódů a ve jmenovateli je hodnota $2^n(2^n - 1)$. Stejný počet je kódů, kde $u_j = u$ a $u_i = u'$, takže pokud chceme, aby platilo $\{u_i, u_j\} = \{u, u'\}$, musíme do jmenovatele dosadit $\binom{2^n}{2}$. Chceme-li pouze, aby $u, u' \in C$, tak je čitatel třeba vynásobit počtem dvojic $\{i, j\}$, tedy hodnotou $\binom{k}{2}$.

Každá dvojice $\{u, u'\} \subseteq \mathbb{F}_2^n$ se proto vyskytuje právě $\sigma$ kódech $C$, kde

$$\sigma = \frac{2^n!\, k(k-1)}{(2^n - k)!\, 2^n(2^n - 1)}.$$

Hodnotu $\sum_C \mu_C(e, \rho)$ můžeme tedy počítat přes všechny dvojice $(u, u')$ z $\mathbb{F}_2^n$, které splňují $u' - u \in S(e, \rho)$ a $u \neq u'$. Takových dvojic je přesně $2^n(V(k, [\rho]) - 1) \leq (2^n - 1)V(k, [\rho]) \leq (2^n - 1)2^{nH(\rho/n)}$, takže $\sum_C \mu_C(e, \rho) \leq \sigma(2^n - 1)2^{nH(\rho/n)}$. Podstatné je, že na pravé straně nefiguruje vektor $e$. Průměrná hodnota výrazu $\frac{1}{k} \sum_{e \in \mathbb{F}_2^n} p^{|e|}(1-p)^{n-|e|} \mu_C(e, \rho)$ počítaná přes všechny kódy je

tedy shora omezena hodnotou

$$\frac{1}{k}\frac{k(k-1)}{2^n(2^n-1)}(2^n-1)2^{nH(\rho/n)}\sum_{e\in\mathbb{F}_2^n}p^{|e|}(1-p)^{n-|e|}.$$

Závěrečná suma je sumou pravděpodobností přes všechny případy, kterých může nabývat chybový vektor $e$, a proto je rovna jedné. Získaný odhad lze tedy zjednodušit na

$$\frac{k-1}{2^n}2^{nH(\rho/n)} < k2^{n(H(p+\eta)-1}.$$

Pro dané $k$ a $\rho$ existuje tedy alespoň jeden kód $C$ o $k$ kódových slovech, pro který

$$\sum_{u'\neq u}\Pr\left(d(u',v)\leq\rho\right) < k2^{n(H(p+\eta)-1}.$$

Abychom důkaz dokončili, vyložíme nyní nejprve, že stačí ověřit, že pro každé $\varepsilon>0$ existují $\alpha<0$ a $\eta>0$ taková, že pro každé dostatečně velké $n$ lze najít celé $k$ tak, že pro $R=(\lg k)/n$ platí

$$1-H(p)-\varepsilon\leq R<1-H(p)\ \text{ a }\ R-1+H(p+\eta)\leq\alpha.$$

Podmínka vlevo je jen zopakováním podmínky na nosnost kódu ze znění Věty 1.1. Podmínka vpravo zaručuje, že

$$k2^{n(H(p+\eta)-1}=2^{Rn}2^{n(H(p+\eta)-1}\leq 2^{\alpha n}$$

se s rostoucím $n$ blíží nule a je tedy od některého $n$ menší než $\delta/2$.

Bez újmy na obecnosti můžeme předpokládat, že $p+\eta<1/2$ a $\varepsilon<1-H(p)$. Hodnotu $\eta$ volíme natolik malou, aby bylo $H(p)+\varepsilon/3\geq H(p+\eta)$. Dále budeme předpokládat, že je $n>3/\varepsilon$. Potom je $n(\varepsilon/3)>1$, takže existuje celé $h$ pro které platí

$$n(1-H(p)-\varepsilon)\leq h\leq n(1-H(p)-2\varepsilon/3).$$

Položme $k=2^h$. Vidíme, že $h=nR$, takže podmínka vlevo splněna je. Splnění druhé podmínky plyne z $h/n\leq 1-H(p)-2\varepsilon/3$, neboť dostáváme

$$R-1+H(p+\eta)\leq H(p+\eta)-H(p)-2\varepsilon/3\leq\varepsilon/3-2\varepsilon/3=-\varepsilon/3.$$

□