Kapitola 7

Kódování

7.1 Opakování z přednášky

Pracujeme nad abecedou $\{0,1\}$. Při použití (n,k)-kódu přenášíme slova o k bitech, kde (na začátek) přidáváme $n-k$ kódových bitů abychom dostali kódová slova o n bitech. *Hammingovou vzdáleností* dvou slov (stejné délky) rozumíme počet bitů, ve kterých se liší.

Věta (28 z přednášky)**.** *Kód* odhaluje r *a méně chyb právě tehdy, když je minimální Hammingova vzdálenost kódových slov alespoň* $r+1$. *Kód* opravuje r *a méně chyb právě tehdy, když je Hammingova vzdálenost kódových slov alespoň* $2\,r+1$.

Lineárním (n,k)*-kódem* rozumíme injektivní lineární zobrazení $g\colon (\mathbb{Z}/2)^k \to (\mathbb{Z}/2)^n$. Ve standardních bázích je reprezentováno $n \times k$ maticí G, které říkáme *generující matice kódu* g. Pokud přidáváme kódové bity na začátek slova, bude mít matice blokový tvar

$$G = \begin{pmatrix} P \\ \mathrm{I}_k \end{pmatrix}. \tag{7.1}$$

Matice P je rozměrů $(n-k) \times k$. Lineární zobrazení $h\colon (\mathbb{Z}/2)^n \to (\mathbb{Z}/2)^{n-k}$, zadané ve standardních bázích maticí

$$H := \begin{pmatrix} \mathrm{I}_{n-k} & P \end{pmatrix} \tag{7.2}$$

o rozměrech $k \times n$, nazýváme *zobrazením kontroly parity* kódu zadaného zobrazením g, matici H pak *maticí kontroly parity* tohoto kódu.

Věta (29 z přednášky)**.** *Nechť lineární kód* g *s generující maticí* G *má zobrazení, respektive matici, kontroly parity* h*, resp.* H*. Potom kódová slova kódu* g *jsou právě* $\ker h$*, tedy slovo* $\mathbf{v}$ *je kódové právě tehdy, když* $h(\mathbf{v}) = 0$.

Pro dané slovo $\mathbf{v} \in (\mathbb{Z}/2)^n$ nazýváme $\mathbf{s} := h(\mathbf{v}) \in (\mathbb{Z}/2)^{n-k}$ *syndromem slova* $\mathbf{v}$, který používáme při dekódování.

Pro dekódování přijatého slova $\mathbf{v}$ si spočítáme jeho syndrom $\mathbf{s}$. Na konec přidáme nuly (počátek $(\mathbb{Z}/2)^k$), získáme slovo $\mathbf{s}|0\ldots0$, které můžeme považovat za bod $(\mathbb{Z}/2)^n$. Přičtením kódových slov získáme afinní podprostor $(\mathbb{Z}/2)^n$ všech chybových slov odpovídajících

syndromu $\mathbf{s}$. Pokud předpokládáme, že při přenosu došlo k nejmenšímu množství chyb, hledáme v tomto podprostoru slovo s nejmenším počtem jedniček, jedničky totiž znamenají odchylku od kódových slov. Hledaným kódovým slovem je pak slovo, z něhož vzniklo přičtením syndromu naše slovo s nejmenším počtem jedniček. Je-li takových slov více, znamená to, že danou chybu neumíme opravit a máme více možností pro kódové slovo a tím i pro původní zprávu.

Jiný způsob dekódování je zakódovat informační bity přijaté zprávy $\mathbf{z}$, čímž vznikne kódové slovo $\mathbf{u}$. Rozdílem $\mathbf{z} - \mathbf{u}$ získáme chybu $\mathbf{e}$. Následně minimalizujeme počet jedniček v $\mathbf{e}$ pomocí sloupců generující matice G. Oba postupy jsou ekvivalentní, jelikož sloupce matice G zadávají bázi $\operatorname{im} g$, tudíž se přičítáním těchto vektorů k bodu $\mathbf{e}$ pohybujeme uvnitř afinního podprostoru chybových slov prináležících syndromu $\mathbf{s}$.

Jedním ze způsobů, jak zadat lineární kód je pomocí polynomů. Polynomy zde zapisujeme seřazené od absolutního členu ke členu vedoucímu. Buď $p(x) = a_0 + a_1\,x + \cdots + {} + a_{n-k}\,x^{n-k}$ polynom stupně $n-k$ nad $\mathbb{Z}/2$. *Polynomiálním kódem* generovaným polynomem p je kód, pro nějž je zobrazením kontroly parity dělení polynomem p se zbytkem. Jedná se o lineární (n, k)-kód. Jeho vstupní slova jsou polynomy nad $\mathbb{Z}/2$ stupně menšího než k, zobrazením g je pak $f \mapsto p \cdot f$, kde f je daný vstupní polynom. Kódovými slovy jsou pak tedy polynomy stupně menšího než n dělitelné polynomem p.

Chceme najít generující matici a matici kontroly parity. Polynomy stupně menšího než $n-k$ lze chápat jako zbytky po dělení polynomem p, tudíž je na nich zobrazení h identita. Matice H je, zapisujeme-li polynomy jako n-tice koeficientů vzestupně vzhledem ke stupni, skutečně tvaru (7.2). Zbývá zjistit, jak vypadá matice P. Sloupce matice H jsou zbytky po dělení polynomů x^i polynomem p, totéž bude platit i pro sloupce matice P. První sloupec bude právě zbytek po dělení p polynomu x^{n-k}, je to tedy sloupec koeficientů členů nižších stupňů polynomu p psaný *zdola nahoru*. Další sloupce jsou zbytky po dělení p monomů vyššího stupně. Ty však dostaneme ze zbytku x^{n-k} vynásobením x, kde případně monom x^{n-k} nahradíme příslušným zbytkem. V praxi tedy posouváme předchozí sloupec *dolů*, na první místo přidáme nulu a při přetečení jedničky nahoře přičítáme *první* sloupec matice P. Je jasné, že pak generující matice bude tvaru (7.1).[1]

7.2 Příklady řešené na cvičení

Příklad 7.1. Množinu čtyř slov chceme přenášet binárním kódem

a) rozpoznávajícím jednoduché chyby;

b) opravujícím jednoduché chyby.

Jakou nejmenší délku slov (chceme pro všechna slova stejnou) můžeme mít? Dejte příklad takových čtyř slov.

[1] Mohli bychom psát matici P i *shora dolů*, ale pak bychom dostali jinou generující matici. Jednalo by se o náš polynomiální kód nikoli ve standardní bázi prostoru polynomů, ale v permutované bázi.

Řešení. Máme slova 00, 01, 10 a 11. Nejprve řešíme a). Potřebujeme, aby minimální Hammingova vzdálenost kódových slov byla 2. Vidíme, že stačí například kód zajišťující sudý počet jedniček. Na začátek přidáme 0 nebo 1 tak, aby byl počet jedniček ve slově vždy sudý. Kódová slova pak budou 000, 101, 110 a 011. Je zřejmé, že se budou lišit minimálně na třech pozicích. Tento kód bude generovaný maticí

$$G_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

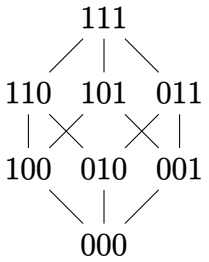
což je lineární $(3, 2)$-kód.

Pro b) potřebujeme, aby byla vzdálenost kódových slov minimálně 3. Jednou možností je opakovat každý bit třikrát. Dostali bychom $(6, 2)$ kód, nicméně přidáváme mnoho bitů. Zkusíme tedy najít nějaký kód, který přidává méně bitů. Můžeme vypozorovat, že vstupní slova mají mezi sebou minimální Hammingovu vzdálenost 1 a kódová slova kódu z a) mají minimální vzdálenost 2. Dáme-li je tedy za sebe kódové slovo z a a vstupní slovo, uvidíme, že se budou nová kódová slova lišite minimálně ve dvou bitech na prvních třech pozicích a v jednom bitu na posledních dvou pozicích, tedy celkem minimálně ve třech bitech. Máme tedy kódová slova 00000, 10101, 11010 a 01111. Jedná se o kódová slova lineárního $(5, 2)$-kódu daného maticí

$$G_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ověřme, že jsou pětibitová kódová slova skutečně minimální délky. Předpokládejme pro spor, že existuje kód s čtyřmístnými kódovými slovy. Bez újmy na obecnosti můžeme předpokládat, že tento kód přidává na bity na začátek kódových slov. Buď $ab00$ kódové slovo odpovídající 00. Pak, má-li se od něj kódové slovo odpovídající 01 lišit na třech pozicích, musí jím být $a'b'01$, kde $(\cdot)'$ značí opačný bit. Tutéž argumentaci lze použít i pro slovo 10, tudíž jsou od sebe kódová slova pro 01 a 10 vzdálena o 1.

Jinak lze řešit úlohu pomocí grafů. Na množinu všech slov délky n se můžeme dívat jako na graf, kde hrana spojuje každé dva vrcholy, které se od sebe liší jen v jednom bitu. Z každého vrcholu tak bude vycházet právě n hran. Graf bude mít tvar n-rozměrné krychle, nebo se na něj můžeme dívat jako na Hasseovský diagram podmnožin n-prvkové množiny (pak n-tice nul a jedniček odpovídají charakteristickým funkcím daných podmnožin). Například pro $n = 3$ budeme mít následující diagram.



Je vidět, že vrcholy 000, 100, 101 a 011 jsou od sebe odděleny vždy minimálně dvěma hranami. Odtud bychom mohli vyřešit a). Vidíme, že pro $n = 3$ máme v krychli dost vrcholů na to, abychom byli schopni najít čtveřici tak, že mezi každými dvěma vrcholy je minimální délka cesty alespoň 2.

Pokud chceme jednoduché chyby i opravovat, potřebujeme minimální délku cest mezi dvěma slovy alespoň 3. To si můžeme přeformulovat na tvrzení: „Pro žádné dva vrcholy v naší čtveřici neexistují jim incidentní hrany se společným druhým vrcholem.“ Pokud $n = 4$, máme celkem 16 vrcholů, 4 z nich jsou naše slova, takže zbývá 12 vrcholů. Jenže z každého z našich vrcholů vedou čtyři hrany do celkem 16 vrcholů, tudíž musí druhé vrcholy některých z nich být společné. Pro $n = 5$ máme celkem 32 vrcholů, 4 kódové, z každého z nich vede 5 hran do celkem 20 vrcholů. Zbývá 28 vrcholů, tedy je jich dost na to, abychom byli schopni najít čtveřici s požadovanou vlastností.

Tento grafový přístup nám umožňuje úlohu zobecnit. Pro dané 2^k hledáme minimální 2^n tak,[2] aby kódová slova délky n odhalovala / opravovala jednoduché chyby. Hledáme minimální n takové, že v n-rozměrné krychli lze najít 2^k vrcholů tak, aby minimální počet hran mezi nimi byl 2, resp. 3.

Má-li být minimální vzdálenost vrcholů 2, stačí vzít $n = k + 1$. To je proto, že $(k+1)$--rozměrná krychle je vlastně dvojice k-rozměrných krychlí, kde „odpovídající si“ vrcholy jsou spojeny hranou. Vezmeme pak z první krychle polovinu vrcholů (od sebe oddělených minimálně 2 hranami), z druhé krychle pak druhou polovinu.

Pro opravování chyb hledáme podobně minimální n tak, abychom v n-rozměrné krychli byli schopni najít 2^k vrcholů tak, že nemají společné žádně druhé vrcholy hran z nich vycházející. Máme celkem 2^n vrcholů, kódových vrcholů je 2^k, z každého z nich vychází n hran. Zbylých vrcholů je $2^n - 2^k$. Potřebujeme, aby mezi nimi bylo alespoň $2^k \cdot n$ vrcholů, neboli

$$2^k \cdot n \leq 2^n - 2^k$$

což odpovídá

$$n - \log_2(n+1) \geq k.$$

Protože je $\mathbb{N}$ dobře uspořádaná množina, má nerovnice pro dané k jediné řešení.[3] △

[2] Vstupní slova musí být nějaké délky, řekněme k, stačí tady úlohu uvažovat v závislosti na délce vstupních a kódových slov.

[3] Alternativně bychom se na nerovnici mohli dívat z druhé strany. Ze slov délky n lze vytvořit kód opravující jednoduché chyby ve slovech maximálně délky $n - \log_2(n+1)$.

Příklad 7.2. Pomocí lineárního kódu daného maticí

$$\left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)$$

zakódujte zprávu 101.

Řešení. Zpráva 101 je sloupcovým vektorem $\mathbf{z} = (1, 0, 1)^{\mathrm{T}}$. Kódování probíhá tak, že daný vektor $\mathbf{z}$ vynásobíme zleva generující maticí G, kde dostaneme vektor

$$\mathbf{k} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

a hledané kódové slovo je 10101. △

Poznámka. Místo násobení sloupcových vektorů zleva jsme mohli také násobit řádkové vektory zprava transponovanou maticí.

Příklad 7.3. Určete všechna kódová slovy $(3, 2)$-kódu generovaného polynomem $x + 1$. Určete generující matici tohoto polynomiálního kódu.

Řešení. Máme polynom $p(x) = 1 + x$. Kód g je dán násobením polynomem p. Vstupní slova budou polynomy $f(x) = a_0 + a_1\, x$, kde a_i, $i \in \{0, 1\}$. Pak

$$g(f)(x) = (p \cdot f)(x) = a_0 + (a_0 + a_1)\, x + a_1\, x^2.$$

Máme čtyři možnosti pro polynom f:

1. $f(x) = 0$: $(p \cdot f)(x) = 0$,
2. $f(x) = 1$: $(p \cdot f)(x) = 1 + x$,
3. $f(x) = x$: $(p \cdot f)(x) = x + x^2$,
4. $f(x) = 1 + x$: $(p \cdot f)(x) = 1 + x + x + x^2 = 1 + x^2$.

Polynom f reprezentuje slovo $a_0 a_1$, podobně pro kódový polynom. Vstupní i kódová slova si můžeme zapsat do následující tabulky

vstupní slovo	00	01	10	11
kódové slovo	000	011	110	101

Vidíme, že všechna kódová slova obsahují sudý počet jedniček. Kód g je skutečně kódem zajišťujícím sudý počet jedniček. Nám zvyklé vyjádření, kde kódový bit přidáváme na začátek slova má pak tento kód například v bázi $(x, 1, x^2)$.

Zobrazení h přiřazuje polynomu stupně 2 zbytek po dělení $p(x) = 1 + x$. Hledáme zbytek po dělení p polynomu $x^{3-2} = x$. Platí

$$x = (1 + x) \cdot 1 + 1$$

tedy zbytek je 1. Zbytek polynomu x^2 je pak x, které si nahradíme 1. Máme tedy matici

$$P = \begin{pmatrix} 1 & 1 \end{pmatrix},$$

matici kontroly parity

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

a generující matici

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

Příklad 7.4. Určete generující matici a matici kontroly parity $(7, 2)$-kódu generovaného polynomem $p(x) = x^5 + x^4 + x^2 + 1$. Dekódujte přijaté slovo 00101|11 za předpokladu, že při přenosu došlo k nejmenšímu možnému množství chyb.

Řešení. Nejprve si zjistíme matici P. Jejím prvním sloupcem bude (vzestupně seřazený) zbytek po dělení x^5 polynomem p. Je vidět, že to bude $x^4 + x^2 + 1$, neboli $(1\,0\,1\,0\,1)^{\mathrm{T}}$. Druhým sloupcem pak bude $(x^4 + x^2 + 1) \cdot x = x^5 + x^3 + x$, kde si x^5 nahradíme zbytkem, tedy vyjde $x^4 + x^3 + x^2 + x + 1$. Pak vyjde matice

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

z čehož získáme matici H přidáním I_5 blokově na první sloupec, tedy

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

a matici G přidáním I_2 blokově na druhý řádek, tedy

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

Dekódujme zprávu 00101|11, která odpovídá vektoru $\mathbf{v} = (0\,0\,1\,0\,1\,1\,1)^{\mathrm{T}}$. Máme dvě možnosti, jak úlohu řešit. Informační bity přijaté zprávy jsou 11. Zakódujeme si zprávu $(1\,1)^{\mathrm{T}}$. Dostaneme kódové slovo $\mathbf{u} = (0\,1\,0\,1\,0\,1\,1)^{\mathrm{T}}$, následně si spočítáme chybu přenosu $\mathbf{e} = \mathbf{v} - \mathbf{u} = (0\,1\,1\,1\,1\,0\,0)^{\mathrm{T}}$. Prvních 5 bitů chybového vektoru je totožných se syndromem zprávy $\mathbf{v}$:

$$\mathbf{s} = H \cdot \mathbf{v} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Nyní se snažíme minimalizovat počet jedniček chyby $\mathbf{e}$ pomocí sloupců generující matice G. Přičtením druhého sloupce G získáme nový chybový vektor $\mathbf{e}' = (1\,0\,0\,0\,0\,0\,1)^{\mathrm{T}}$. Je vidět, že přičtením prvního nebo druhého sloupce matice G k $\mathbf{e}'$ by se počet jedniček zvýšil. Původní zprávu získáme přičtením minimální chyby $\mathbf{e}'$ k přijaté zprávě $\mathbf{v}$, dostaneme zprávu $(1\,0\,1\,0\,1\,1\,0)^{\mathrm{T}}$, tedy původní odeslaná informace byla 10.

Jinou možností je použít metody lineární geometrie. Již jsme si spočítali syndrom $\mathbf{s}$ zprávy $\mathbf{v}$. V $(\mathbb{Z}/2)^7$ si spočítáme obraz kódu g (sestávající z kódových slov). Píšeme-li vstupní slova jako sloupce matice, bude její násobek zleva G odpovídat matici kódových slov. Složenými závorkami značíme, že sloupce matice jsou právě vstupní / kódová slova, jedná se tedy spíše o množinu / prostor sloupcových vektorů, než o matici.

$$G \cdot \left\{ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \left\{ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\},$$

Obraz kódu g tvoří vektorový podprostor v $(\mathbb{Z}/2)^7$. Afinní podprostor chybových slov se syndromem $\mathbf{s}$ dostaneme přičtením vektoru $(\mathbf{s}\,0\,0)^{\mathrm{T}}$, což dává (s přihlédnutím k notaci se

složenými závorkami jako výše)

$$\begin{pmatrix}0\\1\\1\\1\\1\\0\\0\end{pmatrix} + \left\{\begin{matrix}0&1&1&0\\0&1&0&1\\0&1&1&0\\0&1&0&1\\0&1&1&0\\0&0&1&1\\0&1&0&1\end{matrix}\right\} = \left\{\begin{matrix}0&1&1&0\\1&0&1&0\\1&0&0&1\\1&0&1&0\\1&0&0&1\\0&0&1&1\\0&1&0&1\end{matrix}\right\}.$$

Nyní v množině chybových slov hledáme to s nejmenší chybou, tedy sloupec s nejmenším počtem jedniček. V prvním sloupci máme 4 jedničky, ve druhém 2, ve třetím 3 a ve čtvrtém opět 4. Vidíme, že musíme vzít druhý slupec. Poslaná zpráva odpovídala součtu druhého sloupce s obdrženou zprávou, tedy

$$(1\,0\,0\,0\,0\,0\,1)^{\mathrm{T}} + (0\,0\,1\,0\,1\,1\,1)^{\mathrm{T}} = (1\,0\,1\,0\,1\,1\,0)^{\mathrm{T}}$$

což odpovídá zprávě 10101|10 a původní slovo bylo 10. △

Příklad 7.5. Určete generující matici a matici kontroly parity $(7,4)$-kódu generovaného polynomem x^3+x+1. Dekódujte přijatá slova 100|1001 a 101|0110 za předpokladu, že při přenosu došlo k nejmenšímu možnému množství chyb.

Řešení. Zjistíme si matici P. Zbytek po dělení x^3 polynomem x^3+x+1 je $x+1$. Zbytek x^4 je x^2+x, zbytek x^5 je x^3+x^2, který si převedeme na x^2+x+1, a nakonec zbytek x^6 je x^4+x^3, který ji převedeme na $x^2+x+x+1=x^2+1$. Psaním koeficientů zbytků zdola nahoru do sloupců (tedy koeficient u x^2 na poslední řádek, u x na prostřední a u 1 na horní) získáme matici

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

z ní matici kontroly parity

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

a generující matici

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

Obdrželi jsme zprávu 100|1001. Informační bity jsou 1001, zakódujeme si tedy vektor $(1\,0\,0\,1)^{\mathrm{T}}$ maticí G.

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

Chybu přenosu obdržíme odečtením výsledku od obdržené zprávy.

$$\mathbf{e} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Přičtením třetího sloupce matice G snížíme počet jedniček a dostaneme novou chybu

$$\mathbf{e}' = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Vidíme, že přičtením libovolného sloupce matice G by se počet jedniček zvýšil. Chyba $\mathbf{e}'$ je tedy minimální, původní zprávu dostaneme přičtením této minimální chyby k přijaté zprávě:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

a odeslaná zpráva byla 100|1011, tedy původní slovo bylo 1011.

Obdrželi jsme druhou zprávu 101|0110. Zakódujeme si slovo 0110 kódem g.

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

Chybu získáme odečtením od kódového slova od přijaté zprávy.

$$\mathbf{e} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Vidíme, že přičtením libovolného sloupce matice G k chybě $\mathbf{e}$ by se počet jedniček zvýšil. Můžeme proto rovnou říci, že je chyba minimální a původní zpráva byla

$$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

a poslané slovo bylo 0110. To je dáno tím, že dojde-li k (jednoduché) chybě na kódových bitech, je výsledná chyba již minimální.

Chceme-li řešit úlohu pomocí lineární algebry, spočítáme si nejprve množinu kódových slov, kde konvence se závorkami je stejná, jako v příkladu 7.4.

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \left\{ \begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix} \right\} =$$

$$= \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \right\} \quad (7.3)$$

Spočítáme si syndrom první přijaté zprávy 100|1001.

$$\mathbf{s}_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Ten si doplníme nulami na konci a zjistíme afinní podprostor chybových slov syndromu $\mathbf{s}_1$ přičtením k lineárnímu podprostoru kódových slov.

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \left\{ \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \right\} =$$

$$= \left\{ \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \right\}$$

Mezi danými chybovými slovy si najdeme to s nejmenším počtem jedniček, což je v našem případě třetí sloupec, tedy minimální chyba je $(0\,0\,0\,0\,0\,1\,0)^{\mathrm{T}}$ a původní zprávu 100|1011 jsme získali přičtením minimální chyby ke zprávě přijaté.

Nyní si spočítáme syndrom druhé přijaté zprávy 101|0110.

$$\mathbf{s}_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Doplníme jej nulami a přičteme k němu lineární podprostor kódových slov z (7.3), abychom získali afinní podprostor chybových slov daného syndromu.

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \left\{ \begin{matrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix} \right\} =$$

$$= \left\{ \begin{matrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix} \right\}$$

Vidíme, že nejmenší počet jedniček má první chybové slovo, takže odečtením tohoto chybového slova od obdržené zprávy dostaneme

$$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

a poslaná zpráva byla 001|0110, původní informace 0110. △