Kódování

Mgr. Alena Gollová, Dr.

Text k přednášce Teorie informace a kódování, FEL ČVUT, 2012.

Obsah

1 Počítání modulo n **1**

2 Lineární algebra nad $\mathbb{Z}_p$ **3**

3 Lineární kódy **4**

4 Počítání modulo polynom **8**

5 Cyklické kódy **13**

6 Konečná tělesa **16**

7 Polynomy nad $\mathbb{Z}_\mathbf{p}$ a jejich kořeny v tělese T charakteristiky p **21**

8 Kořeny cyklických kódů, BCH-kódy **24**

1 Počítání modulo n

Algebraické struktury - terminologie

1.1 Definice Na množině A je dána binární operace $*$, tj. zobrazení z $A \times A$ do A.

Dvojice $(A, *)$ se nazývá *pologrupa*, pokud je operace $*$ asociativní,
tj. jestliže pro každé $x, y, z \in A$ platí $x * (y * z) = (x * y) * z$.

Dvojice $(A, *)$ se nazývá *monoid*, pokud je operace $*$ asociativní a má neutrální prvek,
tj. jestliže existuje $e \in A$ tak, že pro každé $x \in A$ platí $e * x = x = x * e$.

Dvojice $(A, *)$ se nazývá *grupa*, pokud je operace $*$ asociativní, má neutrální prvek a má všechny inverzní prvky,
tj. jestliže pro každé $x \in A$ existuje $y \in A$ tak, že $x * y = e = y * x$.
Poznámka: Inverzní prvek k prvku x je určen jednoznačně, pokud vůbec existuje, a značíme jej x^{-1}.

Pologrupa, monoid či grupa jsou *komutativní*, pokud je operace $*$ komutativní,
tj. jestliže pro každé $x, y \in A$ platí $x * y = y * x$.

1.2 Definice Mějme množinu A se dvěma binárními operacemi, které označíme jako sčítání a násobení.

Trojice $(A, +, \cdot)$ se nazývá *okruh*, jestliže

- $(A, +)$ je komutativní grupa s neutrálním prvkem 0;
- $(A, \cdot)$ je pologrupa;
- platí oba distributivní zákony,
  tj. pro všechna $x, y, z \in A$ platí $x \cdot (y + z) = x \cdot y + x \cdot z$ a také $(y + z) \cdot x = y \cdot x + z \cdot x$.

Je-li navíc pologrupa $(A, \cdot)$ komutativní, říkáme, že se jedná o *komutativní okruh*; má-li pologrupa $(A, \cdot)$ jednotkový prvek, mluvíme o *okruhu s jednotkou*.

Trojice $(A, +, \cdot)$ se nazývá *těleso*, jestliže je to okruh s jednotkou 1, kde každý nenulový prvek má inverzní prvek, tedy $(A - \{0\}, \cdot)$ je grupa, a kde navíc $0 \neq 1$, tedy neutrální prvek 1 pro násobení není současně neutrálním prvkem 0 pro sčítání.

Většinou budeme říkat stručně těleso, ale půjde o *komutativní těleso*, tj. násobení bude komutativní.

Konstrukce faktorových okruhů modulo n

Vycházíme z množiny celých čísel s operacemi sčítání a násobení. $(\mathbb{Z}, +, \cdot)$ je komutativní okruh s jednotkou, invertibilními prvky jsou v něm pouze 1 a -1. V celých číslech umíme dělit se zbytkem a díky tomu můžeme vystavět celou následující teorii.

1.3 Věta o dělení se zbytkem *Pro každé $a, b \in \mathbb{Z}$, kde $b \neq 0$, existují jednoznačně určené $r, z \in \mathbb{Z}$ tak, že*

$$a = rb + z \quad \text{a} \quad 0 \leq z < b.$$

První sada důsledků:

1.4 Lze definovat *relaci dělitelnosti*: $a|b$ iff $b = ka$ pro nějaké $k \in \mathbb{Z}$. Tato relace je uspořádáním (reflexivní, antisymetrickou a tranzitivní relací) na $\mathbb{N}$. Není však antisymetrická na $\mathbb{Z}$, tam má smysl mluvit o *relaci asociovanosti*: $a||b$ iff $a|b$ a $b|a$; přitom platí, že $a||b$ jen, když $b = \pm a$.

1.5 Můžeme zavést pojem prvočíslo a rozkládat celá čísla na součin prvočísel. Celé číslo $p \geq 2$ je *prvočíslo*, jestliže je dělitelné pouze čísly 1 a p, aneb jestliže se nedá napsat jako součin dvou čísel menších než p. Test prvočíselnosti "hrubou silou": Číslo n je prvočíslo, pokud není dělitelné beze zbytku žádným prvočíslem do $\sqrt{n}$.

1.6 Základní věta aritmetiky Každé celé číslo $n \geq 2$ lze jednoznačně (až na pořadí) napsat jako součin mocnin různých prvočísel.

Druhá sada důsledků:

1.7 Definice *Největší společný dělitel* dvou čísel $a, b \in \mathbb{Z}$ je takové číslo $d \in \mathbb{Z}$, že d dělí obě čísla a i b, d je dělitelné všemi společnými děliteli obou čísel a konečně $d > 0$. Značíme $d = \gcd(a, b)$.

1.8 Největšího společného dělitele lze najít pomocí **Eukleidova algoritmu**. Jedná se o rekurzivní algoritmus, který se opírá o dělení se zbytkem. Předpokládejme, že $a > b$. Podělíme se zbytkem: $a = rb + z$ a $0 \leq z < b$. Pokud je zbytek $z = 0$, tak je $\gcd(a, b) = b$. Pokud je zbytek $z > 0$, tak se snadno dokáže, že dvojice a, b má stejné společné dělitele jako dvojice b, z, tedy i $\gcd(a, b) = \gcd(b, z)$. Budeme dále hledat $\gcd(b, z)$ stejným postupem. Jelikož zbytky jsou celočíselné, nezáporné a stále menší, bude po konečném počtu kroků zbytek nulový a úlohu pro nalezení gcd vyřešíme přímo.

1.9 Věta (Bezoutova) *Největší společný dělitel čísel $a, b \in \mathbb{Z}$ je jejich celočíselnou kombinací, aneb*

$$\gcd(a, b) \;=\; ka \;+\; lb \quad \text{pro} \quad k, l \in \mathbb{Z}.$$

K nalezení celočíselných koeficientů k, l lze použít rozšířený Eukleidův algoritmus. V každém kroku Eukleidova algoritmu přepočítáme aktuální zbytek na kombinaci čísel a a b. Jelikož $\gcd(a, b)$ je posledním nenulovým zbytkem, tak jednou nakombinujeme z čísel a a b i jejich největšího společného dělitele.

1.10 Diofantické rovnice Rovnice $ax + by = c$, kde $a, b, c \in \mathbb{Z}$, má řešení v $\mathbb{Z}$ právě, když $\gcd(a, b)|c$.
Pokud nějaké celočíselné řešení Diofantické rovnice existuje, pak je jich nekonečně mnoho a jsou tvaru

$$(x, y) = (x_p, y_p) + k(x_0, y_0) \quad \text{pro} \quad k \in \mathbb{Z},$$

kde (x_p, y_p) je partikulární řešení a najdeme ho pomocí rozšířeného Eukleidova algoritmu a kde (x_0, y_0) je nesoudělné řešení homogenní rovnice, tedy $(x_0, y_0) = (\frac{b}{d}, -\frac{a}{d})$, kde $d = \gcd(a, b)$.

Třetí sada důsledků:

1.11 Definice Čísla $a, b \in \mathbb{Z}$ jsou *kongruentní modulo* n pro $n \in \mathbb{N}$, jestliže $n|(b - a)$. To nastává právě, když mají čísla a a b stejný zbytek po dělení číslem n. Značíme $a \equiv b \pmod{n}$.

1.12 Tvrzení *Relace kongruence modulo n je relace ekvivalence (reflexivní, symetrická a tranzitivní relace) na množině celých čísel, která je zachována při sčítání a násobení, tj. pokud $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$, pak $a + c \equiv b + d \pmod{n}$ i $ac \equiv bd \pmod{n}$.*

1.13 Relace kongruence modulo n tudíž rozbije množinu celých čísel na třídy navzájem ekvivalentních prvků, tzv. zbytkové třídy modulo n. Množinu zbytkových tříd modulo n značíme $\mathbb{Z}_n$,

$$\mathbb{Z}_n = \mathbb{Z}/\equiv (\text{mod } n) = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$

kde $[a]_n = \{a + kn | k \in \mathbb{Z}\}$.
Na množině $\mathbb{Z}_n$ můžeme korektně definovat operace sčítání a násobení přes representanty:

$$[a]_n \oplus [b]_n = [a + b]_n, \quad [a]_n \odot [b]_n = [a \cdot b]_n$$

Díky definici přes representanty zdědí operace $\oplus$ a $\odot$ vlastnosti, které měly operace sčítání a násobení na $\mathbb{Z}$. Trojice $(\mathbb{Z}_n, \oplus, \odot)$ tvoří komutativní okruh s jednotkou, nazývá se *faktorový okruh modulo n*. V dalším textu zjednodušíme jeho značení na $(\mathbb{Z}_n = \{0, 1, \ldots, n-1\}, +, \cdot)$.

1.14 V okruhu $\mathbb{Z}_n$ umíme řešit lineární rovnice $ax = b$ převedením na Diofantickou rovnici $ax + ny = b$. Víme tedy, že řešení existuje právě, když $\gcd(a, n)|b$, pak $x = x_p + kx_0$, kde $x_0 = \frac{n}{\gcd(a,n)}$. V okruhu $\mathbb{Z}_n$ tak vznikne celkem $\gcd(a, n)$ různých řešení.
Speciálně, pokud řešíme rovnici $ax = 1$ v $\mathbb{Z}_n$, bude řešení existovat jen, když $\gcd(a, n) = 1$, a pak bude toto řešení jediné. Prvek a je invertibilní v $\mathbb{Z}_n$ právě, když a je nesoudělné s n.

1.15 Věta *Okruh $(\mathbb{Z}_n, +, \cdot)$ je těleso právě, když $n = p$ je prvočíslo.*

2 Lineární algebra nad $\mathbb{Z}_p$

2.1 Soustavy lineárních rovnic budeme řešit pouze nad $\mathbb{Z}_p$, kde p je prvočíslo. Zde funguje Gaussova eliminační metoda s tím rozdílem, že místo dělení budeme násobit inverzními prvky (ty existují v $\mathbb{Z}_p$ pro všechny nenulové prvky). Nad $\mathbb{Z}_n$, kde n není prvočíslo, Gaussova eliminační metoda nefunguje.

Všechna řešení homogenní soustavy tvoří podprostor v $\mathbb{Z}_p^n$. Každé řešení nehomogenní soustavy je součtem partikulárního řešení této soustavy a nějakého řešení přidružené homogenní soustavy.
Soustava m lineárních rovnic o n neznámých může mít nad $\mathbb{Z}_p$ žádné řešení, jedno řešení (jedinou n-tici), nebo p^k řešení, kde k je počet proměnných, které smíme volit libovolně v $\mathbb{Z}_p$.

2.2 Maticový počet lze dělat i nad $\mathbb{Z}_n$, ale záležitosti související s Gaussovou eliminací se tam budou chovat jinak, než jak to známe u reálných matic (např hodnost matice $\mathbb{A}^T$ se nemusí rovnat hodnosti matice $\mathbb{A}$).
Matice $\mathbb{A}$ je *regulární matice* nad $\mathbb{Z}_n$, když $\det \mathbb{A}$ je invertibilní v $\mathbb{Z}_n$. Tehdy a jen tehdy existuje inverzní matice k matici $\mathbb{A}$ a lze spočítat jako $\mathbb{A}^{-1} = (\det \mathbb{A})^{-1}\mathbb{D}^T$, kde $\mathbb{D}$ je matice algebraických doplňků k matici $\mathbb{A}$, $\mathbb{D} = (d_{ij}) = ((-1)^{i+j} \det \mathbb{A}_{ij})$, a kde podmatice $\mathbb{A}_{ij}$ vznikla z $\mathbb{A}$ vyškrtnutím i-tého řádku a j-tého sloupce.

2.3 Definice *Lineární prostor* nad tělesem $(T, +, \cdot)$ je množina L spolu s operací sčítání $\oplus : L \times L \to L$ a číselného násobku $\boxdot : T \times L \to L$ (číselný násobek ovšem není binární operace na množině L!), pro které platí:

- $(L, \oplus)$ je komutativní grupa s neutrálním prvkem $\bar{o}$;
- Pro všechny $\alpha, \beta \in T$ a všechny $\bar{u}, \bar{v} \in L$:
  - $\alpha \boxdot (\bar{u} \oplus \bar{v}) = (\alpha \boxdot \bar{u}) \oplus (\alpha \boxdot \bar{v})$
  - $(\alpha + \beta) \boxdot \bar{u} = (\alpha \boxdot \bar{u}) \oplus (\beta \boxdot \bar{u})$
  - $(\alpha \cdot \beta) \boxdot \bar{u} = \alpha \boxdot (\beta \boxdot \bar{u})$
  - $1 \boxdot \bar{u} = \bar{u}$

Prvky lineárního prostory se nazývají vektory, prvky tělesa jsou skaláry. Operace budeme opět značit jen $\cdot$ a $+$.

Množina všech uspořádaných n-tic ze $\mathbb{Z}_p$, tj. $\mathbb{Z}_p^n = \{\bar{u} = (u_1, \ldots, u_n),\ u_i \in \mathbb{Z}_p\}$, spolu se sčítáním a číselným násobkem definovanými po složkách, $\bar{u} + \bar{v} = (u_1 + v_1, \ldots, u_n + v_n)$, $\alpha \cdot \bar{u} = (\alpha u_1, \ldots, \alpha u_n)$, tvoří lineární prostor nad tělesem $\mathbb{Z}_p$. Budeme mu říkat *lineární prostor všech slov délky n nad $\mathbb{Z}_p$*.
Na tomto prostoru lze definovat *skalární součin* předpisem $\bar{u} \odot \bar{v} = u_1 v_1 + \ldots u_n v_n$ a tudíž zde můžeme mluvit o kolmosti vektorů: $\bar{u} \perp \bar{v}$ právě, když $\bar{u} \odot \bar{v} = 0$.

2.4 *Podprostor* lineárního prostoru je neprázdná podmnožina, která je uzavřená na sčítání a číselné násobky. Podprostor musí vždy obsahovat nulový vektor daného prostoru. Nás budou zajímat především podprostory v lineárním prostoru všech slov délky n nad $\mathbb{Z}_p$.

Jsou dvě možnosti, jak jednoznačně popsat podprostor P v lineárním prostoru $\mathbb{Z}_p^n$. První možnost je zvolit v něm nějakou bázi (tj. generující lineárně nezávislou množinu vektorů v P). Pak v podprostoru P jsou jen ty vektory, které se dají nakombinovat z bázických vektorů:

$$\vec{u} \in P \quad \text{iff} \quad \bar{u} = \sum_{i=1}^{k} \alpha_i \bar{b}_i,$$

kde $B = \{\bar{b}_1, \ldots, \bar{b}_k\}$ je báze podprostoru P a $\dim P = k$.

Druhá možnost je najít takovou homogenní soustavu lineárních rovnic, aby množinou všech jejích řešení byl právě podprostor P. Přitom vektor $\bar{u}$ řeší homogenní soustavu $\mathbb{A}\bar{x}^T = \bar{o}^T$ právě, když $R_i \odot \bar{u} = 0$ pro každý řádek R_i matice $\mathbb{A}$, aneb když jsou všechny řádky matice $\mathbb{A}$ kolmé na vektor $\bar{u}$. Hledaná soustava musí mít v řádcích bázi ortogonálního doplňku k podprostoru P:

$$\vec{u} \in P \quad \text{iff} \quad \vec{u} \text{ řeší soustavu } \mathbb{A}\bar{x}^T = \bar{o}^T \text{ s maticí } \mathbb{A} = \begin{pmatrix} \bar{c}_1 \\ \vdots \\ \bar{c}_{n-k} \end{pmatrix},$$

kde $\bar{c}_1, \ldots, \bar{c}_{n-k}$ tvoří bázi podprostoru $P^\perp$.
Díky tomu, že $(P^\perp)^\perp = P$, můžeme naopak určit vektory $\bar{c}_1, \ldots, \bar{c}_{n-k}$ jako bázi podprostoru všech řešení soustavy $\mathbb{B}\bar{x}^T = \bar{o}^T$, kde v řádcích matice $\mathbb{B}$ jsou bázické vektory $\bar{b}_1, \ldots, \bar{b}_k$ podprostoru P.

3 Lineární kódy

Budeme studovat tzv. bezpečnostní kódy, tedy kódy, které umožňují odhalit, zda při přenosu nedošlo k chybě, případně také chybu opravit. Pojem kód bude znamenat množinu všech kódových slov.
Kód délky n nad $\mathbb{Z}_p$ je blokový kód, jehož všechna slova mají stejnou délku n. Abeceda je p-znaková množina $\mathbb{Z}_p$, na které je definována struktura tělesa. Množina všech slov délky n nad $\mathbb{Z}_p$ tudíž tvoří lineární prostor nad tělesem $\mathbb{Z}_p$. Můžeme použít i jiné konečné těleso T (viz následující přednáška) a lineární prostor T^n a vše bude fungovat analogicky.

3.1 Definice Kód K délky n nad $\mathbb{Z}_p$ je *lineární kód*, pokud K tvoří podprostor v lineárním prostoru $\mathbb{Z}_p^n$. Je-li $\dim K = k$, pak mluvíme o lineárním (n, k)-kódu nad $\mathbb{Z}_p$.

Ukážeme záhy, že k určuje počet znaků, které nesou informaci, tzv *informačních znaků*, zatímco zbylých $m = n - k$ znaků je přidáno navíc, abychom mohli objevit nebo dokonce opravit chybu, jsou to tzv. *kontrolní znaky.*

3.2 Příklad Opakovací kód délky 3 nad $\mathbb{Z}_2$ má kódová slova (000) a (111) a jeho (systematické) kódování přiřadí jednomu informačnímu znaku a kódové slovo (aaa). Dva znaky jsou kontrolní a umožňují objevit dvě chyby a opravit jednu chybu (které písmeno je v přijatém slově vícekrát, to považujeme za poslané).

Kódování

3.3 Kódování je zobrazení φ, které každému informačnímu slovu přiřadí slovo kódové. Kódování je dáno volbou báze v podprostoru K. Každý kód tudíž může mít více způsobů, jak informační slova zakódovat.

$$\varphi : \mathbb{Z}_p^k \to K : \bar{a} = (a_1 \dots a_k) \to \bar{v} = \sum_{i=1}^{k} a_i \bar{b}_i, \quad \text{kde } B = \{\bar{b}_1, \dots, \bar{b}_k\} \text{ je báze v K.}$$

Informační znaky tedy jsou souřadnice kódového slova $\bar{v}$ vůči bázi B (a jejich počet $k = \dim K$). To zaručuje, že zobrazení φ je vzájemně jednoznačné. Všimněme si, že lineární (n, k)-kód nad $\mathbb{Z}_p$ má p^k kódových slov.

Generující matice kódu K je matice $\mathbb{G} = \begin{pmatrix} \bar{b}_1 \\ \vdots \\ \bar{b}_k \end{pmatrix}$, která má v řádcích bázická slova kódu K.
Kódování se pak provádí vynásobením maticí $\mathbb{G}$, tj. $\varphi : \bar{a} \to \bar{a} \cdot \mathbb{G} = \bar{v}$.

3.4 Dekódování slova $\bar{v} \in K$ (coby inverzní zobrazení φ^{-1}) spočívá v tom, že nalezneme souřadnice kódového slova $\bar{v}$ vůči bázi, která je v řádcích matice $\mathbb{G}$ použité při zakódování. Musíme tedy řešit soustavu n lineárních rovnic o k neznámých $\mathbb{G}^T \bar{a}^T = \bar{v}^T$, přičemž víme, že $\operatorname{hod} \mathbb{G}^T = k$ a že soustava má řešení (neboť $\bar{v} \in K$). Můžeme se tedy omezit na k lineárně nezávislých rovnic a vyřešit tuto podsoustavu s regulární maticí (např. tak, že ji vynásobíme inverzní maticí).
Nejsnadněji se ale dekóduje, pokud víme, že prvních k znaků kódového slova je slovo informační.

3.5 Systematické kódování je kódování, které ponechá informační znaky na začátku kódového slova a přidá k nim znaky kontrolní, tj. $\varphi : \bar{a} \to \bar{v} = (a_1 \dots a_k b_1 \dots b_{n-k})$. Odpovídá volbě takové báze v kódu K, aby $\mathbb{G} = (\, \mathbb{E}_k \, \mathbb{B} \,)$.
Jelikož je $\operatorname{hod} \mathbb{G} = k$, lze vždy Gaussovou eliminací na řádky matice $\mathbb{G}$ vyrobit generující matici $\mathbb{G}'$ s jednotkovou podmatici $\mathbb{E}_k$, pouze není zaručeno, že sloupce $\mathbb{E}_k$ budou za sebou na začátku matice $\mathbb{G}'$. Gaussova eliminace na řádky matice $\mathbb{G}$ totiž převádí jednu bázi podprostoru K na jiné báze téhož podprostoru K, takže upravená $\mathbb{G}'$ je generující maticí stejného kódu K.

3.6 Tvrzení *Ke každému lineárnímu kódu lze najít systematický kód, který se liší pouze v pořadí znaků. (Systematický kód je kód, který má systematické kódování.)*

3.7 Příklad Koktavý kód délky 6 nad $\mathbb{Z}_2$, $K = \{(a\,a\,b\,b\,c\,c), a, b, c \in \mathbb{Z}_2\}$, je lineární kód, který nemá systematické kódování. Jeho generující matice $\mathbb{G} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$ se nedá úpravami Gaussovy eliminace převést na matici $\mathbb{G}' = (\,\mathbb{E}_3\,\mathbb{B}\,)$. Permutací znaků ale lze udělat systematický kód $K_1 = \{(a\,b\,c\,a\,b\,c), a, b, c \in \mathbb{Z}_2\}$.

Objevování a opravování chyb

Připomeňme nejdříve obecné pojmy, které lze zavést pro všechny blokové kódy. Přitom se podíváme, jak se dá pro objevování a opravování chyb využít skutečnosti, že kód tvoří lineární podprostor.

3.8 Definice *Hammingova váha* $\|\bar{u}\|_H$ slova $\bar{u}$ je rovna počtu nenulových znaků ve slově $\bar{u}$.
Hammingova vzdálenost $d_H(\bar{u}, \bar{v})$ slov $\bar{u}$ a $\bar{v}$ délky n je rovna počtu míst, ve kterých se obě slova liší, aneb $d_H(\bar{u}, \bar{v}) = \|\bar{v} - \bar{u}\|_H$.
Hammingova vzdálenost kódu K je rovna nejmenší Hammingově vzdálenosti různých slov v kódu K, tj. $d_H(K) = \min\{d_H(\bar{u}, \bar{v}) \,|\, \bar{u}, \bar{v} \in K, \bar{u} \neq \bar{v}\}$.

3.9 Tvrzení *Je-li kód K lineární, pak Hammingova vzdálenost kódu je rovna nejmenší Hammingově váze nenulového slova, tj. $d_H(K) = \min\{\|\bar{u}\|_H \,|\, \bar{o} \neq \bar{u} \in K\}$.*

Důkaz Označme $d_H(K) = d$. Pokud pro $\bar{u}, \bar{v} \in K$ je zrovna $d_H(\bar{u}, \bar{v}) = d$, pak slovo $\bar{w} = \bar{v} - \bar{u}$ je kódové, neboť lineární kód K je uzavřen na součty a rozdíly, a má váhu $\|\bar{w}\|_H = d$. Slovo menší váhy v kódu K být nemůže, neboť $\|\bar{u}\|_H = d_H(\bar{u}, \bar{o}) \geq d$, protože lineární kód K obsahuje $\bar{o}$. ⊠

Bylo-li vysláno slovo $\bar{v}$ a přijato slovo $\bar{w} = \bar{v} + \bar{e}$, pak $\bar{e}$ se nazývá *chybové slovo* pro slova $\bar{v}, \bar{w}$.

3.10 Definice Řekneme, že kód K *objevuje chybové slovo* $\bar{e}$, jestliže pro žádné kódové slovo $\bar{v} \in K$ není slovo $\bar{v} + \bar{e}$ kódové. Řekneme, že kód K *objevuje* t chyb, jestliže objevuje každé chybové slovo váhy $\|\bar{e}\|_H \leq t$.

3.11 Tvrzení *Lineární kód K objevuje právě ta chybová slova, která nejsou kódovými slovy.*

3.12 Důsledek *Pro lineární kód K platí: mají-li všechna nenulová kódová slova váhu $\|\bar{v}\|_H > t$, pak kód K objevuje t chyb.*

Poznámka: Pokud kód neobjevuje t chyb, znamená to, že existuje aspoň jedno chybové slovo váhy t, které kód neobjeví. Jiná chybová slova váhy $\geq t$ kód však objevit může.

3.13 Definice Řekneme, že kód K *opravuje* t chyb, jestliže pro každé kódové slovo $\bar{v} \in K$ a každé chybové slovo $\bar{e}$ váhy $\|\bar{e}\|_H \leq t$ platí: Slovo $\bar{v}$ je kódové slovo s nejmenší Hammingovou vzdáleností od slova $\bar{v} + \bar{e}$ mezi všemi kódovými slovy.

3.14 Tvrzení *Má-li kód K Hammingovu vzdálenost d, pak K objevuje nejvýše $t_1 = d - 1$ chyb a opravuje nejvýše $t_2 = [\frac{d-1}{2}]$ chyb.*

3.15 Pro objevování a opravování chyb využít linearity kódu K. Lineární podprostor je totiž možné jednoznačně popsat soustavou lineárních rovnic:

$$\vec{v} \in K \quad \text{iff} \quad \mathbb{H}\,\bar{v}^T = \bar{o}^T \;\text{ pro }\; \mathbb{H} = \begin{pmatrix} \bar{c}_1 \\ \vdots \\ \bar{c}_{n-k} \end{pmatrix}, \;\text{ kde }\; C = \{\bar{c}_1, \ldots, \bar{c}_{n-k}\} \;\text{ je báze v }\; K^\perp.$$

Matice soustavy $\mathbb{H}$ se nazývá **kontrolní matice** kódu K, má řádcích bázická slova ortogonálního doplňku $K^\perp$.

Kontrola přijatého slova pak probíhá takto: Pokud $\mathbb{H}\,\bar{w}^T \neq \bar{o}^T$, pak přijaté slovo $\bar{w} \notin K$, tedy objevili jsme chybu.

Lineární kód K je jednoznačně určen jak maticí generující, tak maticí kontrolní. Řádky jedné z nich určíme coby bázická řešení homogenní soustavy s druhou maticí. Pro systematickou generující matici lze takto odvodit následující snadný výpočet kontrolní matice:

3.16 Tvrzení *Je-li generující matice* $\mathbb{G} = (\,\mathbb{E}_k\,\mathbb{B}\,)$, *pak kontrolní matice* $\mathbb{H} = (\,-\mathbb{B}^T\,\mathbb{E}_{n-k}\,)$.

3.17 Příklad Opakovací kód délky 3 nad $\mathbb{Z}_p$, $K = \{(aaa), a \in \mathbb{Z}_p\}$, je popsán rovnicemi:

$$\bar{v} \in K \quad \text{iff} \quad \begin{array}{rcl} v_1 & = & v_2 \\ v_1 & = & v_3 \end{array} \quad \text{iff} \quad \begin{array}{rcl} v_1 - v_2 & = & 0 \\ v_1 - v_3 & = & 0 \end{array}$$

Kód K má tedy kontrolní matici $\mathbb{H} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix}$.

3.18 Příklad Binární kód kontroly parity délky n má $(n-1)$ informačních znaků a jeden kontrolní znak doplněný tak, aby celková parita slova byla sudá. Je tedy popsán rovnicí

$$\bar{v} \in K \quad \text{iff} \quad v_1 + v_2 + \ldots + v_n \;=\; 0 \quad \text{v } \mathbb{Z}_2$$

a má kontrolní matici $\mathbb{H} = (\,1 \quad 1 \quad \ldots \quad 1\,)$.
Analogicky lze udělat kód kontroly parity délky n nad $\mathbb{Z}_p$, je popsaný rovnicí "součet písmen v kódovém slově je roven nule v $\mathbb{Z}_p$".

3.19 K **opravování chyb** lze také použít kontrolní matici $\mathbb{H}$. Předpokládejme, že posláno bylo kódové slovo $\bar{v}$ a přijato slovo $\bar{w} = \bar{v} + \bar{e}$. Slovo $\bar{s}$, pro nějž je $\bar{s}^T = \mathbb{H}\,\bar{w}^T$ se nazývá *syndrom* přijatého slova $\bar{w}$.

3.20 Tvrzení *Přijaté slovo má stejný syndrom jako jeho chybové slovo. Tento syndrom je kombinací těch sloupců matice* $\mathbb{H}$, *které odpovídají nenulovým pozicím v chybovém slově,* $\bar{s}^T = \sum_{e_i \neq 0} e_i S_i$.

Důkaz $\mathbb{H}\,\bar{w}^T = \mathbb{H}\,(\bar{v} + \bar{e})^T = \mathbb{H}\,\bar{v}^T + \mathbb{H}\,\bar{e}^T = \bar{o}^T + \mathbb{H}\,\bar{e}^T$, neboť $\bar{v} \in K$. Zbytek je jen rozepsané maticové násobení. ⊠

3.21 Speciálně, předpokládejme, že přenosový kanál je bezpečný a že chyba je téměř vyloučena, aneb že ve slově $\bar{w}$ je nejvýše jedna chyba. Pak $\mathbb{H}\,\bar{w}^T = \bar{o}^T$ znamená, že slovo $\bar{w}$ je kódové a považujeme ho za poslané slovo, tedy $\bar{v} = \bar{w}$. V případě jedné chyby na i-té pozici bude $\mathbb{H}\,\bar{w}^T = aS_i$. Určíme-li jednoznačně a a i, můžeme chybu opravit: $\bar{v} = \bar{w} - \bar{e}$, kde $e_i = a$ a $e_j = 0$ pro $j \neq i$.
Toto pozorování má dva bezprostřední důsledky, které v následujícím tvrzení zobecníme:

- Lineární kód objevuje 1 chybu, pokud jeho kontrolní matice $\mathbb{H}$ neobsahuje nulový sloupec.
- Lineární kód opravuje 1 chybu, pokud žádný sloupec jeho kontrolní matice $\mathbb{H}$ není číselným násobkem jiného sloupce v $\mathbb{H}$.

3.22 Tvrzení *Lineární kód* K *objevuje* t *chyb (a opravuje* $[\frac{t}{2}]$ *chyb) právě, když je každých* t *sloupců jeho kontrolní matice* $\mathbb{H}$ *lineárně nezávislých.*

Důkaz Pokud je každých t sloupců v matici $\mathbb{H}$ lineárně nezávislých, tj. žádná jejich netriviální kombinace není rovna nulovému vektoru, pak každé chybové slovo váhy nejvýše t má nenulový syndrom, bude tedy objeveno. ⊠

3.23 Důsledek Lineární (n, k)-kód může objevovat maximálně tolik chyb, kolik má kontrolních znaků. Sloupce matice $\mathbb{H}$ mají délku $n - k$ a proto $n - k + 1$ sloupců je už lineárně závislých.
Je třeba volit kompromis mezi požadavkem objevovat co nejvíce chyb a požadavkem přidávat co nejméně kontrolních znaků.

Hammingovy kódy

3.24 Binární Hammingovy kódy jsou kódy opravující jednu chybu, které mají co nejmenší redundanci (tj. mají co největší počet informačních znaků při daném počtu kontrolních znaků).

Kontrolní matice binárního Hammingova kódu s m kontrolními znaky má ve sloupcích právě všechny nenulové m-tice nad $\mathbb{Z}_2$. Nad $\mathbb{Z}_2$ totiž platí, že dva sloupce jsou lineárně nezávislé právě, když jsou různé. Hammingův kód tedy objevuje dvě chyby a opravuje jednu chybu. Protože jsme do sloupců daly všechny nenulové m-tice nad $\mathbb{Z}_2$, budou kódová slova mít co nejdelší možnou délku umožňující ještě opravování jedné chyby.
Pro $m = 3$ má kontrolní matice Hammingova kódu nad $\mathbb{Z}_2$ tvar:

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

Opravování jedné chyby je navíc u binárních Hammingových kódů velmi snadné. Můžeme si sloupce představit jako binární rozvoje čísel 1 až $(2^m - 1)$ a seřadit je vzestupně. V případě, že syndrom přijatého sloba je binárním rozvojem čísla i, bude chyba na i-té pozici a opravíme ji změnou i-tého znaku na opačný v $\mathbb{Z}_2$.

Délka binárního Hammingova kódu s m kontrolními znaky je $n = 2^m - 1$, počet informačních znaků je tedy $k = 2^m - 1 - m$. Informační poměr $k : n$ roste rychle k 1. Pro $m = 3$ je $k : n = 4 : 7$, pro $m = 6$ je $k : n = 57 : 63$.

3.25 Rozšířený Hammingův kód nad $\mathbb{Z}_2$ obsahuje slova Hammingova kódu prodloužená o znak celkové kontroly parity. Délka slov je tedy $n = 2^m$, počet informačních znaků zůstává $k = 2^m - 1 - m$ a kontrolní matice má tvar

$$\mathbb{H}_R = \begin{pmatrix} & & & 0 \\ & \mathbb{H} & & \vdots \\ & & & 0 \\ 1 & 1 & \dots & 1 \end{pmatrix},$$

kde $\mathbb{H}$ je matice příslušného Hammingova kódu. Prvních $(n-1)$ znaků kódového slova splňuje stejných m rovnic jako u Hammingova kódu a přidaná $(m+1)$-ní rovnice zaručuje sudou paritu kódového slova.
Rozšířený Hammingův kód objevuje 3 chyby (neboť součet libovolných tří sloupců není nulový sloupec) a opravuje jednu chybu.

4 Počítání modulo polynom

"Co se vyplatilo jednou, vyplatí se i podruhé."

V této kapitole zavedeme polynomy nad $\mathbb{Z}_p$ a ukážeme, že množina všech polynomů nad $\mathbb{Z}_p$ tvoří komutativní okruh s jednotkou. Je-li p prvočíslo, tak lze v tomto okruhu dělit se zbytkem každým nenulovým polynomem. Díky tomu můžeme, podobně jako v okruhu celých čísel, vytvořit faktorové okruhy modulo polynom. Počítáme-li modulo ireducibilní polynom, získáme komutativní těleso.

Polynomy nad $\mathbb{Z}_p$

4.1 Definice *Polynom $a(x)$ nad $\mathbb{Z}_p$* je výraz tvaru $a_k\,x^k + \ldots + a_1\,x + a_0$, kde koeficienty a_i jsou ze $\mathbb{Z}_p$. Symbol x nazýváme *proměnná*. Největší k takové, že $a_k \neq 0$, se nazývá *stupeň polynomu*, značí se $\mathrm{st}(a(x))$. Pro nulový polynom klademe $\mathrm{st}(0) = -1$. Množinu všech polynomů nad $\mathbb{Z}_p$ v proměnné x značíme $\mathbb{Z}_p[x]$.

4.2 Definice *Rovnost polynomů nad $\mathbb{Z}_p$* nastane, pokud oba polynomy mají stejný stupeň a stejné koeficienty u stejných mocnin.

Poznámka: Různé polynomy nad $\mathbb{Z}_p$ mohou určovat stejné funkce ze $\mathbb{Z}_p$ do $\mathbb{Z}_p$. Funkce jsou stejné tehdy, mají-li stejný definiční obor a dávají-li stejné výsledky v každém prvku definičního oboru. Je tedy p^p funkcí ze $\mathbb{Z}_p$ do $\mathbb{Z}_p$, zatímco polynomů nad $\mathbb{Z}_p$ je spočetně mnoho. Např. polynomy $x+1$ a x^2+1 určují stejné funkce ze $\mathbb{Z}_2$ do $\mathbb{Z}_2$.

4.3 Na množině polynomů nad $\mathbb{Z}_p$ jsou definovány *operace sčítání* a *násobení* analogicky jako pro reálné polynomy, pouze s koeficienty počítáme v $\mathbb{Z}_p$.

Pro stupně výsledných polynomů platí:

- $\mathrm{st}(a(x) + b(x)) \leq \max(\mathrm{st}(a(x)), \mathrm{st}(b(x)))$
- $\mathrm{st}(a(x) \cdot b(x)) = \mathrm{st}(a(x)) + \mathrm{st}(b(x))$, jsou-li oba polynomy nenulové, jinak by byl $\mathrm{st}(a(x) \cdot b(x)) = -1$.

Poznámka: Pro polynomy nad $\mathbb{Z}_n$, kde $n \neq p$, neplatí tento vztah pro stupeň součinu, protože okruh $\mathbb{Z}_n$ obsahuje dělitele nuly (tj. nenulové prvky, jejichž součin je nula). Např. v $\mathbb{Z}_6[x]$ je $\mathrm{st}(2x \cdot 3x) = \mathrm{st}(0) = -1$.

4.4 Tvrzení *Trojice $(\mathbb{Z}_p[x], +, \cdot)$ tvoří komutativní okruh s jednotkou. Invertibilními jsou v něm pouze nenulové konstanty.*

4.5 Věta o dělení se zbytkem *Pro libovolné polynomy $a(x), b(x) \in \mathbb{Z}_p[x]$, kde $b(x) \neq 0$, existují jednoznačně určené polynomy $r(x), z(x) \in \mathbb{Z}_p[x]$ tak, že*

$$a(x) = r(x)\,b(x) + z(x) \quad \text{a} \quad \mathrm{st}(z(x)) < \mathrm{st}(b(x)).$$

Důkaz Polynomy $r(x)$ a $z(x)$ najdeme stejným algoritmem pro dělení polynomů jako u reálných polynomů, pouze místo dělení vedoucím koeficientem používáme násobení k němu inverzním prvkem.
Pro $\mathrm{st}(a(x)) < \mathrm{st}(b(x))$ je $r(x) = 0$ a $z(x) = a(x)$. V opačném případě spočteme první člen částečného podílu takto:

$$(a_k\,x^k + \ldots + a_1\,x + a_0) : (b_m\,x^m + \ldots + b_1\,x + b_0) = (a_k\,b_m^{-1}\,x^{k-m} + \ldots \quad)$$

Po zpětném vynásobení polynomu $b(x)$ prvním členem podílu a po odečnení tohoto součinu od polynomu $a(x)$ se sníží stupeň dělence. Postup opakujeme, dokud není stupeň dělence menší než $\mathrm{st}(b(x))$. ⊠

Poznámka: V algoritmu dělení polynomů je důležité, že jakýkoliv nenulový vedoucí koeficient polynomu $b(x)$ má v tělese $\mathbb{Z}_p$ inverzní prvek. To v okruhu $\mathbb{Z}_n$ neplatí, tudíž algoritmus dělení nebude pro polynomy, jejichž vedoucí koeficient nemá inverzní prvek, fungovat. Skutečně, v $\mathbb{Z}_n[x]$, kde n není prvočíslo, nelze dělit těmi polynomy, které mají neinvertibilní vedoucí koeficient. Tudíž pro polynomy nad $\mathbb{Z}_n$ nelze vystavět následující teorii opřenou o dělení se zbytkem. Naopak algoritmus dělení polynomů funguje pro polynomy nad libovolným tělesem T, pro ně se dá následující teorie zcela analogicky použít.

První sada důsledků:

4.6 Definice Polynom $a(x)$ *dělí* polynom $b(x)$ v $\mathbb{Z}_p[x]$, jestliže $b(x) = r(x)\,a(x)$ pro nějaký polynom $r(x) \in \mathbb{Z}_p[x]$. Značíme $a(x) \,|\, b(x)$.

Přitom nenulová konstanta c ze $\mathbb{Z}_p$ dělí každý polynom $b(x)$, neboť $b(x) = c \cdot (c^{-1}b(x))$. Relace dělitelnosti není uspořádáním na množině $\mathbb{Z}_p[x]$. Polynomy, které se liší o konstantní násobek, se dělí navzájem, tj. $a(x) \,|\, b(x)$ a $b(x) \,|\, a(x)$. Říkáme, že jsou to *asocionané polynomy*, a značíme $a(x) \,||\, b(x)$.

4.7 Definice Prvek $c \in \mathbb{Z}_p$ je *kořen* polynomu $q(x) \in \mathbb{Z}_p[x]$, jestliže platí $q(c) = 0$.

4.8 Tvrzení *Prvek $c \in \mathbb{Z}_p$ je kořenem polynomu $q(x) \in \mathbb{Z}_p[x]$ právě, když polynom $(x - c)$ dělí polynom $q(x)$.*

4.9 Tvrzení *Polynom $q(x) \in \mathbb{Z}_p[x]$ stupně $k \geq 0$ má v tělese $\mathbb{Z}_p$ nejvýše k kořenů.*

Důkaz indukcí podle k. Polynom stupně nula je nenulová konstanta, nemá tedy žádný kořen. Předpokládejme, že každý polynom stupně k má nejvýše k kořenů, a zvolme libovolně polynom $q(x)$ stupně $k + 1$. Pokud $q(x)$ nemá žádný kořen, tak počet kořenů je menší než $k + 1$. Pokud má $q(x)$ kořen c, tak $q(x) = (x - c)\,r(x)$, kde $\mathrm{st}(r(x)) = k$, tudíž dle předpokladu má polynom $r(x)$ nejvýše k kořenů. Přitom pro libovolný kořen b polynomu $q(x)$ platí $0 = q(b) = (b - c)\,r(b)$ v tělese $\mathbb{Z}_p$. Protože těleso nemá dělitele nuly, je buď $b = c$ nebo $r(b) = 0$, tj. b je kořen polynomu $r(x)$. Počet kořenů polynomu $q(x)$ je tudíž nejvýše $k + 1$. ⊠

Poznámka: Stejně by se dokázalo, že polynom nad libovolným tělesem má nejvýše tolik kořenů, kolik je jeho stupeň. Důkaz však selže pro polynomy nad okruhem, ve kterém jsou dělitelé nuly. Tam je skutečně možné, že polynom stupně k má více než k kořenů a že se dá rozložit různými způsoby na polynomy nižších stupňů. Např. v $\mathbb{Z}_8[x]$ platí $x^2 - 1 = (x - 1)(x + 1) = (x - 3)(x + 3)$. Polynom $x^2 - 1$ má celkem čtyři kořeny v okruhu $\mathbb{Z}_8$ a jsou to prvky $1, -1 = 7, 3, -3 = 5$.

4.10 Definice Polynom $q(x)$ stupně $k \geq 1$ se nazývá *ireducibilní* polynom nad $\mathbb{Z}_p$, jestliže se $q(x)$ nedá napsat jako součin dvou polynomů nad $\mathbb{Z}_p$ stupně menšího než k.

Každý polynom lze rozložit na $q(x) = c \cdot (c^{-1}q(x))$ pro $0 \neq c \in \mathbb{Z}_p$, stejně jako lze každé celé číslo rozložit na $n = 1 \cdot n$. Ireducibilní polynomy $q(x)$ má pouze tyto rozklady, aneb $q(x)$ je dělitelný pouze konstantami a polynomy asociovanými s $q(x)$.

4.11 Testování ireducibility polynomu $q(x)$: Polynom $q(x)$ je ireducibilní nad $\mathbb{Z}_p$, pokud není dělitelný žádným ireducibilním polynomem nad $\mathbb{Z}_p$ stupně nejvýše $\frac{\mathrm{st}(q(x))}{2}$.

Místo dělení polynomu $q(x)$ lineárními polynomy $(x - c)$ můžeme zkoušet, zda c není kořenem polynomu $q(x)$.

4.12 Tvrzení *Polynom $q(x)$ stupně $\mathrm{st}(q) \leq 3$ je ireducibilní nad $\mathbb{Z}_p$ právě, když $q(x)$ nemá kořen v $\mathbb{Z}_p$.*

4.13 Příklad Polynom x^2+1 je ireducibilní nad $\mathbb{Z}_3$, neboť nemá kořen v $\mathbb{Z}_3$. Tentýž polynom je ale rozložitelný nad $\mathbb{Z}_2$, neboť má kořen $c = 1$ v $\mathbb{Z}_2$, $x^2 + 1 = (x + 1)^2$ je jeho rozklad na ireducibilní polynomy v $\mathbb{Z}_2[x]$.
Polynom $x^4 + x^2 + 1$ sice nemá kořen v $\mathbb{Z}_2$, ale není ireducibilní, neboť $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ v $\mathbb{Z}_2[x]$.

4.14 Věta *Nad $\mathbb{Z}_p$ existují ireducibilní polynomy libovolného stupně $k \geq 1$.*

Uvědomme si, že situace s ireducibilními polynomy je nad $\mathbb{Z}_p$ naprosto jiná než u reálných polynomů. Mezi reálnými polynomy jsou kromě lineárních polynomů ireducibilní už jen kvadratické polynomy s komplexně sdruženými kořeny a všechny reálné polynomy stupně $k \geq 3$ jsou rozložitelné.

4.15 Tvrzení *Každý polynom $m(x)$ nad $\mathbb{Z}_p$ lze jednoznačně (až na pořadí) rozložit v $\mathbb{Z}_p[x]$ na součin konstanty a monických ireducibilních polynomů, tj. $m(x) = c \cdot q_1(x) \cdot \ldots \cdot q_n(x)$, kde $c \in \mathbb{Z}_p$ a všechny q_i jsou monické polynomy ireducibilní nad $\mathbb{Z}_p$ (monické polynomy mají vedoucí koeficient roven 1).*

Poznámka: Jednoznačnost rozkladů platí pro polynomy na libovolným tělesem, nemusí však platit pro polynomy nad okruhem, jak bylo ukázáno výše.

Druhá sada důsledků:

4.16 Definice *Největší společný dělitel* dvou polynomů $a(x), b(x) \in \mathbb{Z}_p[x]$ je takový polynom $d(x) \in \mathbb{Z}_p[x]$, že $d(x)$ dělí oba polynomy $a(x)$ i $b(x)$, že $d(x)$ je dělitelný všemi společnými děliteli obou polynomů a konečně že $d(x)$ je monický polynom (má vedoucí koeficient roven 1). Značíme $d(x) = \gcd(a(x), b(x))$.

Bez požadavku, aby největší společný dělitel byl monický, bychom měli celou třídu navzájem asociovaných největších společných dělitelů polynomů $a(x)$ a $b(x)$. Připusťme i tento pohled na věc.

4.17 Definice Polynomy jsou *nesoudělné*, pokud jejich největší společný dělitel je 1 (nebo nenulová konstanta, nebudeme-li požadovat monický největší společný dělitel).

4.18 Pro hledání největšího společného dělitele polynomů můžeme použít **Eukleidovův algoritmus**, protože se opírá pouze o dělení se zbytkem a v okruhu polynomů nad $\mathbb{Z}_p$ dělit se zbytkem umíme. Tudíž funguje i rozšířený Eukleidův algoritmus, který dokazuje Bezoutovu větu.

4.19 Věta (Bezoutova) *Největší společný dělitel $a(x), b(x) \in \mathbb{Z}_p[x]$ je jejich polynomiální kombinací,*

$$\gcd(a(x), b(x)) \;=\; k(x)a(x) \;+\; l(x)b(x) \quad \text{pro} \quad k(x), l(x) \in \mathbb{Z}_p[x].$$

4.20 Polynomiální rovnice $a(x)r(x) + b(x)s(x) = c(x)$, kde $a(x), b(x), c(x) \in \mathbb{Z}_p[x]$, má řešení v $\mathbb{Z}_p[x]$ právě, když $\gcd(a(x), b(x)) \mid c(x)$ v $\mathbb{Z}_p[x]$. Pokud nějaké řešení existuje, pak je jich nekonečně mnoho a jsou tvaru

$$(r(x), s(x)) = (r_p(x), s_p(x)) + k(x)(r_0(x), s_0(x)) \quad \text{pro} \quad k(x) \in \mathbb{Z}_p[x],$$

kde $(r_p(x), s_p(x))$ je partikulární řešení a najdeme ho pomocí rozšířeného Eukleidova algoritmu a kde $(r_0(x), s_0(x))$ je nesoudělné řešení homogenní rovnice, tedy $(r_0(x), s_0(x)) = (\frac{b(x)}{d(x)}, -\frac{a(x)}{d(x)})$ pro $d(x) = \gcd(a(x), b(x))$.

Třetí sada důsledků:

Konstrukce faktorových okruhů modulo polynom

4.21 Definice Polynomy $a(x), b(x) \in \mathbb{Z}_p[x]$ jsou *kongruentní modulo polynom* $m(x)$, jestliže $m(x) \mid (b(x) - a(x))$ v $\mathbb{Z}_p[x]$. Značíme $a(x) \equiv b(x) \pmod{m(x)}$.

4.22 Tvrzení *$a(x) \equiv b(x) \pmod{m(x)}$ právě, když mají $a(x)$ a $b(x)$ stejný zbytek po dělení polynomem $m(x)$.*

4.23 Tvrzení *Relace kongruence modulo polynom $m(x)$ je relace ekvivalence (tj. reflexivní, symetrická a tranzitivní relace) na množině všech polynomů nad $\mathbb{Z}_p$, která je zachována při sčítání a násobení:*
Pokud $a(x) \equiv b(x) \pmod{m(x)}$ a $c(x) \equiv d(x) \pmod{m(x)}$,
pak $a(x) + c(x) \equiv b(x) + d(x) \pmod{m(x)}$, a $a(x) \cdot c(x) \equiv b(x) \cdot d(x) \pmod{m(x)}$.

4.24 Relace kongruence modulo polynom $m(x)$ tudíž rozbije množinu polynomů nad $\mathbb{Z}_p$ na třídy navzájem ekvivalentních polynomů, tj. třídy $[a(x)]_{m(x)} = \{a(x) + k(x)m(x) \mid k(x) \in \mathbb{Z}_p[x]\}$. Polynomy v jedné třídě mají stejný zbytek po dělení polynomem $m(x)$, můžeme jej tedy zvolit za representanta této třídy. Třídy nazýváme zbytkové třídy modulo polynom $m(x)$. Množinu všech zbytkových tříd modulo $m(x)$ značíme $\mathbb{Z}_p[x]/m(x)$.
Má-li polynom $m(x)$ stupeň k, pak zbytkem po dělení $m(x)$ může být jakýkoliv polynom nad $\mathbb{Z}_p$ stupně menšího než k, je tedy celkem p^k různých zbytkových tříd.

$$\mathbb{Z}_p[x]/m(x) = \{[a(x)]_{m(x)}, a(x) \in \mathbb{Z}_p[x],\ \mathrm{st}(a(x)) < \mathrm{st}(m(x))\}$$

Na množině $\mathbb{Z}_n$ můžeme korektně definovat operace sčítání a násobení přes representanty:

$$[a(x)]_{m(x)} \oplus [b(x)]_{m(x)} = [a(x) + b(x)]_{m(x)}, \quad [a(x)]_{m(x)} \odot [b(x)]_{m(x)} = [a(x) \cdot b(x)]_{m(x)}$$

Díky definici přes representanty zdědí operace $\oplus$ a $\odot$ vlastnosti, které měly operace sčítání a násobení na polynomech nad $\mathbb{Z}_p$.

4.25 Tvrzení *Trojice* $(\mathbb{Z}_p[x]/m(x), \oplus, \odot)$ *tvoří komutativní okruh s jednotkou, tzv. faktorový okruh modulo polynom* $m(x)$.

V dalším textu zjednodušíme značení: pro prvky faktorových okruhů budeme používat jinou proměnnou než x, místo $[a(x)]_{m(x)}$ budeme psát většinou $a(z)$, násobení a sčítání budeme značit obyčejně $\cdot$ a $+$.

$$(\,\mathbb{Z}_p[x]/m(x) = \{a_{k-1}\,z^{k-1} + \ldots + a_1\,z + a_0,\; a_i \in \mathbb{Z}_p\}, +, \cdot\,)$$

Všimněme si, že sčítání je normálním sčítáním polynomů nad $\mathbb{Z}_p$, při sčítání se totiž nezvýší stupeň a počítání modulo $m(x)$ se neprojeví. Výsledkem násobení je zbytek po dělení součinu polynomů nad $\mathbb{Z}_p$ polynomem $m(x)$.

4.26 Lineární rovnice $a(z)r(z) = b(z)$ ve faktorovém okruhu $\mathbb{Z}_p[x]/m(x)$ řešíme převedením na polynomiální rovnici $a(x)r(x) + m(x)s(x) = b(x)$ v $\mathbb{Z}_p[x]$.
Víme tedy, že řešení existuje právě, když $\gcd(a(x), m(x)) \mid b(x)$. Pak všechna řešení mají tvar

$$r(z) = r_p(z) + k(z)r_0(z), \quad \text{kde} \quad r_0(z) = \frac{m(z)}{d(z)} \quad \text{pro} \quad d(x) = \gcd(a(x), m(x)).$$

Různá řešení v okruhu $\mathbb{Z}_p[x]/m(x)$ budou vznikat pro různé polynomy $k(x) \in \mathbb{Z}_p[x]$ stupně menšího než je $\mathrm{st}(d(x))$.

4.27 Tvrzení *Prvek* $a(z)$ *je invertibilní v okruhu* $\mathbb{Z}_p[x]/m(x)$ *právě, když je polynom* $a(x)$ *nesoudělný s polynomem* $m(x)$ *v* $\mathbb{Z}_p[x]$.

Důkaz Inverzní prvek k $a(z)$ řeší rovnici $a(z)r(z) = 1$. Řešení rovnice existuje jen, když $\gcd(a(x), m(x)) \mid 1$, tedy $a(x)$ je nesoudělný s $m(x)$. ⊠

4.28 Věta *Faktorový okruh* $\mathbb{Z}_p[x]/q(x)$ *je tělesem právě tehdy, když* $q(x)$ *je ireducibilní polynom nad* $\mathbb{Z}_p$.

Důkaz Ireducibilní polynom nemůže být soudělný se žádným polynomem nižšího stupně kromě 0, takže všechny nenulové prvky faktorového okruhu mají inverzní prvek. ⊠

4.29 Definice Nechť $q(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$ stupně k. Těleso $\mathbb{Z}_p[x]/q(x)$ se nazývá *Galoisovo těleso* o p^k prvcích a značí se $GF(p^k)$.

4.30 Pro Galoisova tělesa lze dokázat:

- Pro libovolné prvočíslo p a přirozené číslo k existuje Galoisovo těleso o p^k prvcích (aneb existují ireducibilní polynomy nad $\mathbb{Z}_p$ libovolného stupně k).
- Každá dvě Galoisova tělesa o p^k prvcích jsou izomorfní (aneb na volbě ireducibilního polynomu nezáleží).
- Jiná konečná tělesa než tělesa Galoisova neexistují.

4.31 Příklady

- Okruh $A = \mathbb{Z}_2[x]/(x^2+1) = \{0, 1, z, z+1\}$ není těleso, protože polynom $x^2+1 = (x+1)^2$ není ireducibilní nad $\mathbb{Z}_2$. Konkrétně prvek $z+1$ nemá inverzní prvek.
- Okruh $B = \mathbb{Z}_2[x]/(x^2+x+1) = \{0, 1, z, z+1\}$ je těleso, neboť polynom x^2+x+1 je ireducibilní nad $\mathbb{Z}_2$.

Všimněme si, že okruhy A a B mají stejné prvky a stejné sčítání, liší se pouze násobením. Oba okruhy také obsahují prvky 0 a 1 (resp. [0], [1]) a s nimi se počítá stejně jako v $\mathbb{Z}_2$. Okruh B je navíc tělesem, říkáme, že B je *rozšíření tělesa*, či *nadtěleso* tělesa $\mathbb{Z}_2$.

4.32 Jiný pohled na násobení ve faktorovém okruhu $\mathbb{Z}_\mathbf{p}[\mathbf{x}]/\mathbf{m}(\mathbf{x})$

Nechť $m(x) = a_k x^k + \ldots + a_1 x + a_0$ je polynom je stupně k. V okruhu $\mathbb{Z}_p[x]/m(x)$ platí vztah

$$m(z) = a_k z^k + \ldots + a_1 z + a_0 = 0,$$

protože vydělíme-li polynom $m(x)$ sebou samým, dostaneme zbytek 0. Z této rovnosti můžeme vyjádřit

$$z^k = a_k^{-1}(-a_{k-1} z^{k-1} - \ldots - a_1 z - a_0).$$

Přitom okruh $\mathbb{Z}_p[x]/m(x)$ obsahuje polynomy stupně nejvýše $(k-1)$. Při vynásobení dvou prvků vznikne polynom stupně nejvýše $(2k-2)$. Potřebujeme tedy pravidla pro přepsání mocnin z^k, z^{k+1} až z^{2k-2}, celkem $(k-1)$ přepisovacích pravidel. Přepisovací pravidlo pro z^k jsme již odvodili ze vztahu $m(z) = 0$. Ostatní přepisovací pravidla získáme z tohoto pravidla postupným násobením proměnnou z a dosazováním předchozích pravidel.

Přepisovací pravidla lze použít i k řešení lineárních rovnic $a(z)r(z) = b(z)$ ve faktorovém okruhu $\mathbb{Z}_p[x]/m(x)$. Místo Eukleidova algoritmu budeme muset vyřešit soustavu k lineárních rovnic nad $\mathbb{Z}_p$ pro k neznámých koeficienktů polynomu $r(z)$.

4.33 Příklady

- Okruh $A = \mathbb{Z}_2[x]/(x^2+1) = \{0, 1, z, z+1\}$ má přepisovací pravidlo pro násobení $z^2 = -1$. Bývá zvykem značit $z = i$. Vytvořili jsme komplexní čísla nad $\mathbb{Z}_2$.
- Těleso $B = \mathbb{Z}_2[x]/(x^2+x+1) = \{0, 1, z, z+1\}$ má přepisovací pravidlo pro násobení $z^2 = z + 1$.
- Těleso $T = \mathbb{Z}_2[x]/(x^3+x+1) = \{a\alpha^2 + b\alpha + c,\, a, b, c \in \mathbb{Z}_2\}$ má dvě přepisovací pravidla pro násobení, $\alpha^3 = \alpha + 1$ a $\alpha^4 = \alpha^2 + \alpha$.

4.34 O okruzích $\mathbb{Z}_p[x]/(x^2+1)$ mluvíme též jako o komplexních číslech nad $\mathbb{Z}_p$ a značíme je $\mathbb{Z}_p[i]$. Tedy $\mathbb{Z}_p[i] = \{ai + b,\, a, b \in \mathbb{Z}_p,\, i^2 = -1\}$. Stejným způsobem vznikla i komplexní čísla nad $\mathbb{R}$, $\mathbb{C} = \mathbb{R}[x]/x^2 + 1$. Komplexní čísla nad $\mathbb{Z}_p$ však netvoří vždy těleso, neboť polynom $x^2 + 1$ nemusí být ireducibilní nad $\mathbb{Z}_p$. Např. $\mathbb{Z}_3[i]$ je těleso, ale $\mathbb{Z}_2[i]$ není těleso (viz příklad 4.13).

5 Cyklické kódy

5.1 Definice Lineární kód K délky n nad $\mathbb{Z}_p$ je *cyklický*, pokud je množina kódových slov uzavřená na cyklické posuny, tj. pokud pro každé $\bar{v} = (v_1 v_2 \dots v_n) \in K$ je také $c(\bar{v}) = (v_2 \dots v_n v_1) \in K$.

5.2 Příklad Opakovací kód délky n nad $\mathbb{Z}_p$ je zřejmě cyklický.
Binární kód kontroly parity délky n je cyklický, protože obsahuje právě všechna slova délky n o sudém počtu jedniček a cyklické otáčení počet jedniček nezmění.

5.3 U cyklických kódů se vyplatí chápat kódová slova délky n jako polynomy stupně nejvýše $(n-1)$. Cyklický posun je pak realizován vynásobením proměnnou z podle pravidla $z^n = 1$. Tedy

$$\begin{array}{lcrcl} \bar{v} = (v_1 \dots v_{n-1} v_n) & \leftrightarrow & v(z) & = & v_1 z^{n-1} + \dots + v_{n-1} z + v_n \\ c(\bar{v}) = (v_2 \dots v_n v_1) & \leftrightarrow & z \cdot v(z) & = & v_1 z^n + v_2 z^{n-1} + \dots + v_{n-1} z^2 + v_n z \\ & & & = & v_2 z^{n-1} + \dots + v_{n-1} z^2 + v_n z + v_1 \end{array}$$

Jakožto lineární prostory nad $\mathbb{Z}_p$ se prostor $\mathbb{Z}_p^n$ všech slov nad $\mathbb{Z}_p$ délky n a prostor všech polynomů nad $\mathbb{Z}_p$ stupně nejvýše $(n-1)$ shodují (sčítání a násobení konstantou ze $\mathbb{Z}_p$ je v nich realizováno stejně). Proto budeme prostor polynomů nad $\mathbb{Z}_p$ stupně nejvýše $(n-1)$ značit $\mathbb{Z}_p^{(n)}$.
Na množině všech polynomů nad $\mathbb{Z}_p$ stupně nejvýše $(n-1)$ máme však navíc operaci násobení - umíme vynásobit dva polynomy nad $\mathbb{Z}_p$ a použít přepisovací pravidlo $z^n = 1$ (a další odvozená pravidla $z^{n+1} = z$, $z^{n+2} = z^2$ atd.), takže výsledkem bude opět polynom stupně nejvýše $(n-1)$. Takto definované násobení odpovídá násobení ve faktorovém okruhu $\mathbb{Z}_p[x]/(x^n - 1)$, aneb $\mathbb{Z}_p^{(n)}$ tvoří komutativní okruh s jednotkou.

5.4 Definice Nechť $(R, +, \cdot)$ je komutativní okruh. Podmnožina $I \subset R$ se nazývá *ideál* okruhu R, jestliže $(I, +)$ je podgrupa grupy $(R, +)$ a jestliže pro všechny $r \in R$ a všechny $i \in I$ je $r \cdot i \in I$.

5.5 Tvrzení *Cyklický kód K délky n nad $\mathbb{Z}_p$ je ideál v okruhu $\mathbb{Z}_p^{(n)}$.*

Důkaz Cyklický kód K je lineární, tvoří lineární podprostor v $\mathbb{Z}_p^{(n)}$, a je tudíž podgrupou vůči sčítání. Zbývá dokázat uzavřenost kódu K na násobení libovolným polynomem ze $\mathbb{Z}_p^{(n)}$.
K je cyklický kód, tudíž pro $v(z) \in K$ je $z \cdot v(z) \in K$, a tudíž je také $z^2 \cdot v(z) \in K$ a libovolné $z^i \cdot v(z) \in K$.
Buď $a(z) = \sum_{i=1}^{s} a_i z^i \in \mathbb{Z}_p^{(n)}$, pak $a(z) \cdot v(z) = \sum_{i=1}^{s} a_i (z^i \cdot v(z))$ je lineární kombinací kódových polynomů, ale K je lineární kód, tudíž $a(z) \cdot v(z) \in K$. ⊠

5.6 Definice *Generující polynom* cyklického kódu K nad $\mathbb{Z}_p$ je takový kódový polynom $g(z) \in K$, že každý kódový polynom je jeho polynomiálním násobkem, tj.

$$v(z) \in K \quad \text{iff} \quad v(z) = a(z) \cdot g(z) \quad \text{pro nějaký } a(z) \in \mathbb{Z}_p^{(n)}.$$

5.7 Tvrzení *Každý cyklický kód K délky n nad $\mathbb{Z}_p$ má generující polynom.*

Důkaz Zvolme jako $g(z)$ nějaký nenulový kódový polynom nejmenšího stupně. Dokážeme, že libovolný kódový polynom $v(z) \in K$ je jeho násobkem. Podle věty o dělení polynomů nad $\mathbb{Z}_p$ je $v(z) = a(z) \cdot g(z) + r(z)$, kde $\mathrm{st}(r) < st(g)$. Avšak polynom $r(z) = v(z) - a(z) \cdot g(z)$ je také kódový, neboť K je ideál v $\mathbb{Z}_p^{(n)}$. Protože $g(z)$ má nejmenší stupeň mezi nenulovými kódovými polynomy, musí být $r(z) = 0$. ⊠

5.8 Důkaz předchozího tvrzení nám dává návod, jak najít generující polynom $g(z)$ cyklického kódu K. Je jím jakýkolikv nenulový kódový polynom nejmenšího stupně. Takových polynomů bude právě $(p-1)$ a budou se lišit o vynásobení nenulovou konstantou ze $\mathbb{Z}_p$ (budou to navzájem asociované polynomy).

Dále je z důkazu patrné, že každý kódový polynom je tvaru $v(z) = a(z) \cdot g(z)$, kde $n - 1 \geq \mathrm{st}(v) = \mathrm{st}(a) + \mathrm{st}(g)$ (protože $a(z)$ vznikl dělením), aneb při násobení $a(z) \cdot g(z)$ se nepoužívá přepisovací pravidlo $z^n = 1$ a jde o obyčejné násobení polynomů nad $\mathbb{Z}_p$. Pro různé polynomy $a(z)$ tedy vzniknou různé kódové polynomy $v(z)$ (neboť okruh polynomů nad $\mathbb{Z}_p$ nemá dělitele nuly) a každé kódové slovo vznikne tímto způsobem, tj. vynásobením polynomu $g(z)$ nějakým polynomem $a(z)$ stupně nejvýše $(n - 1 - \mathrm{st}(g))$. Jde o vzájemně jednoznačné přiřazení mezi polynomy $a(z)$ a kódovými polynomy $v(z)$, které určuje kódování informace délky $k = n - \mathrm{st}(g)$.

5.9 Kódování pomocí generujícího polynomu: Nechť K je cyklický (n,k)-kód s generujícím polynomem $g(z)$, tedy $\mathrm{st}(g) = n-k$. Kódování informace délky k probíhá takto: Informačnímu slovu přiřadíme informační polynom stupně nejvýše $(k-1)$, ten vynásobíme generujícím polynomem $g(z)$ a vzniklý kódový polynom stupně nejvýše $(n-1)$ opět přepíšeme na kódové slovo.

$$\begin{array}{rcll} \bar{a} = (a_1 \dots a_{k-1} a_k) & \leftrightarrow & a(z) = a_1\, z^{k-1} + \dots + a_{k-1}\, z + a_k & \\ a(z) & \longrightarrow & v(z) = a(z) \cdot g(z) & \\ & & v(z) = v_1\, z^{n-1} + \dots + v_{n-1}\, z + v_n & \leftrightarrow \quad \bar{v} = (v_1 \dots v_{n-1} v_n) \end{array}$$

Dekódování: Kódový polynom $v(z) \in K$ vydělíme generujícím polynomem $g(z)$ nad $\mathbb{Z}_p$ a získáme informační polynom $a(z) = v(z) : g(z)$.

5.10 Tvrzení *Je-li $g(z)$ generující polynom cyklického (n,k)-kódu K nad $\mathbb{Z}_p$, pak*
1) množina $\{g(z), z\,g(z), z^2\,g(z), \dots, z^{k-1}\,g(z)\}$ tvoří bázi podprostoru K (bázi získáme otáčením slova $\bar{g}$, které odpovídá generujícímu polynomu $g(z)$).
2) Generující matice $\mathbb{G} = \begin{pmatrix} c^{k-1}(\bar{g}) \\ \vdots \\ c(\bar{g}) \\ \bar{g} \end{pmatrix}$ *určuje stejné kódování jako generující polynom $g(z)$.*

Důkaz $v(z) \in K$ iff $v(z) = a(z) \cdot g(z) = \sum_{i=1}^{k} a_i\,(z^i \cdot g(z))$, přitom polynomy $g(z), z\,g(z), \dots, z^{k-1}\,g(z)$ jsou lineárně nezávislé (neboť násobení probíhá v okruhu polynomů nad $\mathbb{Z}_p$), tvoří tedy bázi podprostoru K.
Zapíšeme-li lineární kombinaci maticově, a pak přepíšeme do kódových slov, získáme kódování pomocí matice $\mathbb{G}$.

$$v(z) = a(z) \cdot g(z) = \bar{a} \cdot \begin{pmatrix} z^{k-1} \cdot g(z) \\ \vdots \\ z \cdot g(z) \\ g(z) \end{pmatrix} \leftrightarrow \bar{v} = \bar{a} \cdot \begin{pmatrix} c^{k-1}(\bar{g}) \\ \vdots \\ c(\bar{g}) \\ \bar{g} \end{pmatrix} = \bar{a} \cdot \mathbb{G}$$

⊠

5.11 Příklad Binární kód kontroly parity délky 3 má kódová slova $K = \{(0\,0\,0), (0\,1\,1), (1\,0\,1), (1\,1\,0)\}$ a kódové polynomy $K = \{0, z+1, z^2+1, z^2+z\}$. Generujícím polynomem je $g(z) = z+1$ a určuje toto kódování:

$$\begin{array}{llll} \bar{a} = (0\,0) & \longrightarrow & v(z) = 0 \cdot g(z) = 0 & \leftrightarrow \quad \bar{v} = (0\,0\,0) \\ \bar{a} = (0\,1) & \longrightarrow & v(z) = 1 \cdot g(z) = z+1 & \leftrightarrow \quad \bar{v} = (0\,1\,1) \\ \bar{a} = (1\,0) & \longrightarrow & v(z) = z \cdot g(z) = z^2+z & \leftrightarrow \quad \bar{v} = (1\,1\,0) \\ \bar{a} = (1\,1) & \longrightarrow & v(z) = (z+1) \cdot g(z) = z^2+1 & \leftrightarrow \quad \bar{v} = (1\,0\,1) \end{array}$$

Stejné kódování určuje matice $\mathbb{G} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \leftrightarrow \begin{pmatrix} z \cdot g(z) \\ g(z) \end{pmatrix}$.

5.12 Systematické kódování pro cyklický (n,k)-kód K lze také provádět pomocí generujícího polynomu $g(z)$. Nejprve informačnímu slovu přiřadíme polynom stupně $(n-1)$ tak, že informační znaky napíšeme na začátek (od nejvyšších mocnin):

$$\bar{a} = (a_1 \dots a_k) \longrightarrow u(z) = a_1\, z^{n-1} + a_2\, z^{n-2} + \dots + a_k\, z^{n-k}$$

Polynom $u(z)$ vydělíme generujícím polynomem $g(z)$ a dostaneme:

$$u(z) = f(z)\, g(z) + r(z), \quad \text{kde} \quad st(r) < st(g) = n-k$$

Polynom $v(z) = u(z) - r(z) = f(z)\, g(z)$ je kódový polynom z K, neboť je násobkem generujícího polynomu. Navíc odečítání zbytkového polynomu nezasáhlo do informačních znaků:

$$v(z) = u(z) - r(z) = a_1\, z^{n-1} + a_2\, z^{n-2} + \dots + a_k\, z^{n-k} - r_{n-k-1}\, z^{n-k-1} - \dots - r_1\, z - r_0$$

Přiřadíme-li informačnímu slovu $\bar{a}$ kódové slovo $\bar{v} \leftrightarrow v(z)$, bude toto přiřazení určovat systematické kódování.

5.13 Tvrzení *Generující polynom $g(z)$ cyklického kód K délky n nad $\mathbb{Z}_p$ dělí beze zbytku polynom $x^n - 1$ v polynomech nad $\mathbb{Z}_p$.*

Důkaz Podle věty o dělení polynomů je $x^n - 1 = h(x) \cdot g(x) + r(x)$, kde $\mathrm{st}(r) < \mathrm{st}(g)$ v $\mathbb{Z}_p[x]$. Potom v okruhu $\mathbb{Z}_p^{(n)} = \mathbb{Z}_p[x]/x^n - 1$ je $0 = h(z) \cdot g(z) + r(z)$, odkud $r(z) = -h(z) \cdot g(z) \in K$, neboť K je ideál v $\mathbb{Z}_p^{(n)}$. Protože má generující polynom nejnižší stupeň mezi nenulovými kódovými polynomy, musí být $r(z) = 0$. ⊠

5.14 Důsledek *Každý rozklad polynomu $x^n - 1 = h(x) \cdot g(x)$ v polynomech nad $\mathbb{Z}_p$ určuje cyklický kód délky n nad $\mathbb{Z}_p$. Je tedy tolik cyklických kódů délky n nad $\mathbb{Z}_p$, kolik je monických dělitelů polynomu $x^n - 1$ v $\mathbb{Z}_p[x]$.*

5.15 Příklad V $\mathbb{Z}_2[x]$ je $x^3 - 1 = (x+1)(x^2 + x + 1)$ rozklad na ireducibilní polynomy, existují tedy pouze dva binární cyklické kódy délky 3. Je to opakovací kód s $g(z) = z^2 + z + 1$ a kód kontroly parity s $g(z) = z + 1$.

5.16 Definice *Kontrolní polynom* cyklického kódu K délky n nad $\mathbb{Z}_p$ je takový polynom $h(z) \in \mathbb{Z}_p^{(n)}$, že pro každý polynom $v(z) \in \mathbb{Z}_p^{(n)}$ platí:

$$v(z) \in K \quad \text{iff} \quad v(z) \cdot h(z) = 0 \quad \text{v okruhu} \quad \mathbb{Z}_p^{(n)} = \mathbb{Z}_p[x]/x^n - 1$$

aneb násobení je podle pravidla $z^n = 1$.

5.17 Tvrzení *Každý cyklický kód K délky n nad $\mathbb{Z}_p$ má kontrolní polynom.*

Důkaz Položme $h(x) = (x^n - 1) : g(x)$ v $\mathbb{Z}_p[x]$, kde dělení je beze zbytku dle předchozího tvrzení. Víme, že $v(z) \in K$ právě, když $v(z) = a(z) \cdot g(z)$, což nastane právě, když $v(z) \cdot h(z) = a(z) \cdot g(z) \cdot h(z) = a(z) \cdot (z^n - 1) = 0$, počítáme-li podle pravidla $z^n = 1$. ⊠

Poznámka Pro cyklický (n, k)-kód K nad $\mathbb{Z}_p$ je $\mathrm{st}(h) = k$, protože $h(x) \cdot g(x) = x^n - 1$ v $\mathbb{Z}_p[x]$ a už víme, že $\mathrm{st}(g) = n - k$.

5.18 Tvrzení *Nechť $h(z) = h_k\, z^k + \ldots + h_1\, z + h_0$ je kontrolní polynom cyklického (n, k)-kódu K nad $\mathbb{Z}_p$. Pak kontrolní matice kódu K má tvar*

$$\mathbb{H} = \begin{pmatrix} 0 & \ldots & & 0 & h_0 & h_1 & \ldots & h_k \\ & & & \vdots & & & & \\ 0 & h_0 & h_1 & \ldots & h_k & 0 & \ldots & 0 \\ h_0 & h_1 & \ldots & h_k & 0 & & \ldots & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} z^{n-k-1} \cdot h(z)^{op} \\ \vdots \\ z \cdot h(z)^{op} \\ h(z)^{op} \end{pmatrix},$$

kde $h(z)^{op}$ znamená, že koeficienty polynomu se do slova délky n vypisují v opačném pořadí, tedy od nejnižších mocnin.

Důkaz Při kontrole slova $\bar{w}$ touto maticí $\mathbb{H}$ vznikají v syndromu $\bar{s}^T = \mathbb{H}\, \bar{w}^T$ koeficienty polynomu $h(z) \cdot w(z)$, kontrolou tedy projde slovo $\bar{w}$ právě, když projde polynom $w(z)$. Konkrétně

$$\bar{s}^T = \mathbb{H}\, \bar{w}^T = \begin{pmatrix} s_k \\ \vdots \\ s_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{iff} \quad h(z) \cdot w(z) = s_{n-1}\, z^{n-1} + \ldots + s_k\, z^k + \ldots + s_0 = 0.$$

⊠

5.19 Opravování chyb Pokud je v přijatém polynomu jedna chyba, pak $w(z) = v(z) + a\, z^i$, kde $v(z) \in K$. Při vynásobení kontrolním polynomem vznikne syndrom $w(z) \cdot h(z) = 0 + a\, z^i \cdot h(z)$. Určíme-li jednoznačně a a z^i, pak můžeme chybu opravit: $v(z) = w(z) - a\, z^i$. Ale pozor, násobení jsme prováděli podle pravidla $z^n = 1$, nelze tedy jednoduše podělit syndromový polynom polynomem $h(z)$ jakožto polynomy nad $\mathbb{Z}_p$.

K opravování chyb budeme raději používat kontrolní matici.

6 Konečná tělesa

V této kapitole budeme pod pojmem těleso mít na mysli vždy konečné komutativní těleso, tedy množinu s dvěma binárními operacemi $(T, +, \cdot)$, kde $(T, +)$ je komutativní grupa s neutrálním prvkem 0, $(T - \{0\}, \cdot)$ je komutativní grupa s neutrálním prvkem 1, přičemž $1 \neq 0$, a násobení je distributivní vůči sčítání.

Charakteristika tělesa

6.1 Definice Nechť $(T, +, \cdot, 0, 1)$ je konečné těleso. Nejmenší přirozené číslo $r > 0$ takové, že $\underbrace{1 + 1 + \ldots + 1}_{r\text{-krát}} = 0$, se nazývá *charakteristika tělesa* T. Značíme $\operatorname{char} T$.
(Charakteristika tělesa je vlastně řád prvku 1 v grupě $(T, +)$ - viz následující kapitola.)

6.2 Tvrzení *Charakteristika konečného tělesa je vždy prvočíslo.*

Důkaz Kdyby $\operatorname{char} T = r$ bylo složené číslo, $r = ab$ pro $1 < a \leq b < r$, pak by bylo platilo:

$$0 = \underbrace{1 + 1 + \ldots + 1}_{r\text{-krát}} = \underbrace{\underbrace{(1 + 1 + \ldots + 1)}_{a\text{-krát}} + \ldots + \underbrace{(1 + 1 + \ldots + 1)}_{a\text{-krát}}}_{b\text{-krát}} = \underbrace{(1 + 1 + \ldots + 1)}_{a\text{-krát}} \cdot \underbrace{(1 + 1 + \ldots + 1)}_{b\text{-krát}}$$

(Při úpravách používáme toho, že sčítání je asociativní, 1 je neutrální prvek vůči násobení, násobení je distributivní vůči sčítání.) Protože těleso nemá dělitele nuly, musí být buď $\underbrace{1 + 1 + \ldots + 1}_{a\text{-krát}} = 0$ nebo $\underbrace{1 + 1 + \ldots + 1}_{b\text{-krát}} = 0$, což je spor s tím, že r je nejmenší takové číslo. Tudíž r je prvočíslo. ⊠

6.3 Příklad Zřejmě $\operatorname{char} \mathbb{Z}_p = p$. Nechť $T = \mathbb{Z}_p[x]/q(x)$, kde $q(x)$ je ireducibilní nad $\mathbb{Z}_p$, pak $\operatorname{char} T = p$.
Aneb každé rozšíření T tělesa $\mathbb{Z}_p$ vytvořené jako faktorový okruh polynomů nad $\mathbb{Z}_p$ modulo ireducibilní polynom, má charakteristiku p.

6.4 Ukážeme, že $\operatorname{char} T = p$ právě, když těleso T je rozšířením tělesa $\mathbb{Z}_p$. V následující části opět 1 značí neutrální prvek vůči násobení a 0 značí neutrální prvek vůči sčítání v tělese T.
Množina

$$P = \{1,\ 1 + 1,\ 1 + 1 + 1, \ldots, \underbrace{1 + 1 + \ldots + 1}_{p\text{-krát}} = 0\}$$

má p různých prvků a tvoří podgrupu grupy $(T, +)$ generovanou prvkem 1. Množina P je uzavřená i vůči násobení (součin dvou prvků z P se dá přepsat podle distributivního zákona na součet 1, což je prvek z P), a snadno se odvodí, že P tvoří podtěleso tělesa T.
Podle tvrzení o řádech prvků je $k \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{k\text{-krát}} = 0$ právě, když $p \mid k$, tedy v tělese P se počítá stejně jako v tělese $\mathbb{Z}_p$. Zobrazení

$$\underbrace{1 + 1 + \ldots + 1}_{k\text{-krát}} \longleftrightarrow k$$

je tudíž tělesový izomorfismus, skrze který můžeme ztotožnit těleso $(P, +, \cdot)$ s tělesem $(\mathbb{Z}_p, +, \cdot)$ a psát $\mathbb{Z}_p \subseteq T$. Těleso T charakteristiky p lze považovat za rozšíření tělesa $\mathbb{Z}_p$.

6.5 Tvrzení *Každé konečné těleso má p^k prvků, pro nějaké prvočíslo p a nějaké přirozené číslo k.*

Důkaz Těleso T charakteristiky p lze považovat za lineární prostor nad tělesem $\mathbb{Z}_p$ (násobení skaláry ze $\mathbb{Z}_p$ je realizováno jako násobení v tělese T, neboť $\mathbb{Z}_p \subseteq T$). Jelikož je T konečné těleso, tak musí mít jakožto lineární prostor konečnou bázi, označme $\dim T = k$. Každý prvek z lineárního prostoru T je lineární kombinací k bázických prvků s koeficienty ze $\mathbb{Z}_p$, těchto kombinací je právě p^k. ⊠

Aneb na šestiprvkové množině není možné definovat operace sčítání a násobení tak, aby byly splněny vlastnosti požadované pro komutativní těleso.

6.6 Tvrzení *Nechť T je těleso charakteristiky p. Pak pro každé $a, b \in T$ platí:* $(a+b)^p = a^p + b^p$

Důkaz Podle binomické věty je

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}\, b^k$$

Přitom $\binom{p}{0} = \binom{p}{p} = 1$ a pro $1 \le k \le (p-1)$ je $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p\cdot(p-1)\cdot\ldots\cdot(p-k+1)}{1\cdot2\cdot3\cdot\ldots\cdot k}$. V čitateli je součin k po sobě jdoucích přirozených čísel a ten je vždy dělitelný číslem $k!$. Zlomek lze zkrátit tak, že ve jmenovateli bude 1, přičemž p je prvočíslo, takže p v čitateli zůstane. Pro $1 \le k \le (p-1)$ je tedy $\binom{p}{k} = p \cdot l$, pro $l \in \mathbb{N}$. V tělese charakteristiky p je $\binom{p}{k} = p \cdot l = 0$, všechny mezičleny vypadnou a zůstane $(a+b)^p = a^p + b^p$. ⊠

6.7 Důsledek *Nechť T je těleso charakteristiky p, a nechť $m \in \mathbb{N}$.*
1. Pro každé $a, b, \in T$ je $(a+b)^{(p^m)} = a^{(p^m)} + b^{(p^m)}$.
2. Pro všechny $a_1, \ldots, a_n \in T$ je $(a_1 + a_2 + \ldots + a_n)^{(p^m)} = a_1^{(p^m)} + a_2^{(p^m)} + \ldots + a_n^{(p^m)}$.

Důkaz Lze dokázat z předchocího tvrzení konečnou indukcí dle m, resp. dle n. ⊠

6.8 Tvrzení *Pro polynomy nad $\mathbb{Z}_p$ platí:*
1. $x^p - 1 = (x-1)^p$, tedy prvek $1 \in \mathbb{Z}_p$ je p-násobný kořen polynomu $x^P - 1$.
2. $x^{(p^m)} - 1 = (x-1)^{(p^m)}$, tedy prvek $1 \in \mathbb{Z}_p$ je p^m-násobný kořen polynomu $x^{(p^m)} - 1$.
3. $x^{p-1} - 1 = (x-1)(x-2)\ldots(x-(p-1))$, tedy všechny prvky $0 \ne a \in \mathbb{Z}_p$ jsou kořenem polynomu $x^{p-1} - 1$.

Důkaz
1. Protože $\operatorname{char} \mathbb{Z}_p = p$, lze dokázat obdobně jako v předchozím tvrzení, že $(x-1)^P = x^p + (-1)^p$. Ale $(-1)^p = -1$, neboť prvočíslo p je liché (kromě $p = 2$, ale v $\mathbb{Z}_2$ je $-1 = 1$).
3. Z Malé Fermatovy věty každé $0 \ne a \in \mathbb{Z}_p$ splňuje $a^{p-1} = 1$ v $\mathbb{Z}_p$, je tedy kořenem polynomu $x^{p-1} - 1$. ⊠

Primitivní prvek tělesa

Nejdříve bude třeba připomenout některé výsledky z teorie konečných grup, jako např. pojmy řád prvku v grupě, generátor cyklické grupy, Lagrageovu větu a Eulerovu větu pro konečné grupy. Tyto výsledky ponecháme většinou bez důkazu.

6.9 Věta (Eulerova) *Nechť $(G, \circ, 1)$ je konečná grupa o n prvcích. Pro každé $a \in G$ platí: $a^n = 1$ v G.*

Důkaz (pro komutativní grupu G) Levá translace prvkem $a \in G$ definovaná předpisem $l_a : G \to G : l_a(x) = a \circ x$ je v grupě vzájemně jednoznačné zobrazení. Tudíž součin všech prvků z grupy $G = \{x_1, x_2, \ldots, x_n\}$ je možné napsat dvěma způsoby:

$$s = \prod_{i=1}^{n} x_i = \prod_{i=1}^{n} (a \circ x_i)$$

Díky komutativitě dostáváme

$$s = a^n \circ \prod_{i=1}^{n} x_i = a^n \circ s,$$

a vynásobíme-li rovnost prvkem s^{-1}, který v grupě existuje, získáme dokazovaný vztah $1 = a^n$. ⊠

6.10 Věta (Malá Fermatova) *Pro každé $a \ne 0$ je $a^{p-1} = 1$ v $\mathbb{Z}_p$.*

6.11 Věta (Euler-Fermatova) *Pro každé a nesoudělné s n je $a^{\varphi(n)} = 1$ v $\mathbb{Z}_n$.*

6.12 Uvědomme si, že obě tyto věty jsou speciální verzí Eulerovy věty pro grupu invertibilních prvků v $\mathbb{Z}_n$. Grupu invertibilních prvků v monoidu $(\mathbb{Z}_n, \cdot)$ značíme $\mathbb{Z}_n^*$ a invertibilní jsou právě prvky nesoudělné s n:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n; a \text{ je nesoudělné s } n\}$$

Počet prvků této grupy $|\mathbb{Z}_n^*| = \varphi(n)$, kde φ je Eulerova funkce:

$$\varphi : \mathbb{N} \to \mathbb{N} : \varphi(n) = \text{ počet čísel mezi 0 až (n-1) nesoudělných s n}$$

Pro výpočet Eulerovy funkce platí následující vzorce, na základě kterých umíme spočítat $\varphi(n)$, kdykoli známe prvočíselný rozklad čísla n.

- $\varphi(p) = p - 1$ pro p prvočíslo
- $\varphi(p^k) = p^k - p^{k-1}$ pro p prvočíslo a k přirozené číslo
- $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$ pro n, m navzájem nesoudělná přirozená čísla

Například $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8, \}$, $|\mathbb{Z}_9^*| = \varphi(9) = 6$, všechny prvky $a \in \mathbb{Z}_9$ splňují $a^6 = 1$ v $\mathbb{Z}_9$. Ovšem číslo 6 není vždy ten nejmenší exponent, na který je třeba umocnit, aby vyšlo 1, třeba $8^2 = 1$ a $4^3 = 1$ v $\mathbb{Z}_9$. Tento fakt vede k následující definici.

6.13 Definice Nechť $(G, \circ)$ je konečná grupa s neutrálním prvkem 1, $a \in G$. Nejmenší přirozené číslo $r > 0$ takové, že $a^r = \underbrace{a \circ a \circ \ldots \circ a}_{r\text{-krát}} = 1$ se nazývá *řád prvku* a v grupě G. Značíme $\mathrm{r}(a) = r$.

Takové $r > 0$, že $a^r = 1$, v grupě G určitě existuje. V konečné grupě se musí výsledky mocnin opakovat, $a^k = a^l$ pro nějaké $k < l$. Vynásobíme-li rovnost inverzním prvkem k prvku a^k, který v grupě musí existovat, dostaneme $1 = a^{l-k}$. Definice pojmu řád prvku a je smysluplná.

6.14 Tvrzení *Nechť $(G, \circ, 1)$ je konečná grupa, $a \in G$. Je-li $\mathrm{r}(a) = r$, pak množina $P = \{a, a^2, a^3, \ldots, a^r = 1\}$ tvoří r-prvkovou podgrupu grupy G, tzv. cyklickou podgrupu generovanou prvkem a, značíme ji $P = \langle a \rangle$.*

6.15 Věta (Lagrangeova) *Počet prvků libovolné podgrupy P (v grupě G) je dělitelem počtu prvků grupy G.*

6.16 Důsledek *Řád prvku a v grupě G je dělitelem počtu prvků grupy G.*

6.17 Definice Grupa $(G, \circ, 1)$ o n prvcích se nazývá *cyklická grupa*, pokud $G = \langle a \rangle = \{a, a^2, a^3, \ldots, a^n = 1\}$. Prvek a je tzv. *generátor* grupy G.

6.18 Tvrzení *Prvek a je generátor grupy $(G, \circ, 1)$ o n prvcích právě, když $\mathrm{r}(a) = n$. To nastane právě, když je splněna kterákoliv z následujících podmínek:*

- *$a^r \neq 1$ pro každé $r < n$, kde $r \mid n$*
- *$a^r \neq 1$ pro každé $r = \frac{n}{p}$, kde p je prvočíslo a $p \mid n$*

6.19 Příklad Chceme najít generátor grupy $\mathbb{Z}_{19}^*$, která má $\varphi(19) = 18$ prvků. Možné řády jsou dělitelé čísla $18 = 2 \cdot 3^2$, přičemž maximální dělitelé jsou 6 a 9. Zkusíme $a = 2$ a spočteme $2^6 = 7 \neq 1$ a $2^9 = -1 \neq 1$. Prvek 2 tedy je generátor a grupa $\mathbb{Z}_{19}^*$ je cyklická.

6.20 Tvrzení *Nechť $(G, \circ, 1)$ je konečná grupa, $a \in G$. Pak $a^k = 1$ v grupě G právě, když $r(a) \mid k$.*

6.21 Tvrzení *Nechť $r(a) = r$ v grupě G, pak $r(a^k) = \frac{r}{\gcd(k,r)}$ v grupě G.*
Speciálně, pokud $r(a) = ks$, pak $r(a^k) = s$.

6.22 Nechť $G = \langle a \rangle$ je cyklická grupa o n prvcích. Nechť $r \mid n$, tehdy a jen tehdy platí:

1. V grupě G lze nalézt prvek řádu r, například prvek $b = a^k$, kde $n = kr$.
2. Prvků řádu r je v grupě G celkem $\varphi(r)$ a jsou tvaru b^j pro všechna j nesoudělná s r, $0 \leq j < r$.

3. Rovnice $x^r = 1$ má v grupě G právě r řešení - jsou to všechny prvky z podgrupy $\langle b\rangle$ generované prvkem řádu r. (Tyto prvky jsou tvaru b^i, $0 \le i < r$, tudíž řeší danou rovnici: $(b^i)^r = (b^r)^i = 1^i = 1$, a fakt, že v cyklické grupě žádná další řešení nejsou, plyne z následujícího bodu.)
4. V grupě G je právě jedna podgrupa o r prvcích a to podgrupa $P_r = \langle b\rangle$, kde $b = a^k$ pro $k = \frac{n}{r}$.

Pro obecné r (tedy i když $r \nmid n$ platí:

1. Rovnice $x^r = 1$ má právě $d = \gcd(r, n)$ řešení v grupě G (a to všechny prvky z podgrupy P_d, aneb rovnice se redukuje na $x^d = 1$).

A teď už zpět ke konečným tělesům:

6.23 Věta *Nechť $(T, +, \cdot, 0, 1)$ je konečné těleso o n prvcích. Grupa invertibilních prvků v tělese, tedy grupa $(T^* = T - \{0\}, \cdot)$, je vždy cyklická.*

Důkaz První část důkazu se opírá o vlastnosti řádů prvků. Řád prvku je dělitelem počtu prvků grupy, tedy $r(a) \,|\, (n-1)$. Chceme najít prvek, jehož řád je $n-1$. Označíme jako m největší řád prvků v grupě T^*. Dokážeme, že pak řád libovolného prvku v T^* dělí toto m (což dá trochu práce - musíme dokázat, že existuje-li v grupě prvek řádu r a prvek řádu s, pak v ní existuje i prvek řádu $\mathrm{lcm}(r, s)$). Tudíž každý prvek v T^* splňuje $a^m = 1$ a je kořenem polynomu $x^m - 1$. Druhá část důkazu se opírá o fakt, že v tělese může mít polynom nejvýše tolik kořenů, kolik je jeho stupeň. Odtud $m = n-1$ a každý prvek, který má tento řád m, je generátorem grupy T^*. ☒

6.24 Definice Nechť $(T, +, \cdot, 0, 1)$ je konečné těleso, jakýkoliv generátor grupy $(T^* = T - \{0\}, \cdot)$ se nazývá *primitivní prvek* tělesa T.

6.25 Tvrzení *Nechť T je konečné těleso o n prvcích. Polynom $x^r - 1$ má v tělese T celkem r různých kořenů právě, když $r \,|\, (n-1)$.*

Důkaz Grupa $(T^*, \cdot)$ je cyklická grupa o $(n-1)$ prvcích. V ní existuje prvek β řádu r právě, když $r \,|\, (n-1)$. Tento prvek je kořen polynomu $x^r - 1$, neboť splňuje $\beta^r = 1$. Podgrupa generovaná prvkem β má r prvků tvaru β^i, $1 \le i \le r$, a každý z nich je kořenem polynomu $x^r - 1$, neboť $(\beta^i)^r = (\beta^r)^i = 1^i = 1$. Více kořenů polynom stupně r mít v tělese nemůže. (Aneb kořeny polynomu $x^r - 1$ jsou právě všechna řešení rovnice $x^r = 1$ v cyklické grupě T^*.) Pokud $r \nmid (n-1)$, pak má rovnice $x^r = 1$ v cyklické grupě pouze $\gcd(r, n-1) < r$ řešení, tedy polynomu $x^r - 1$ má méně než r kořenů. ☒

6.26 Věta Fermatova: *Nechť T je konečné těleso o n prvcích. Pak každý prvek tělesa je kořenem polynomu $x^n - x$, tj. pro každý $a \in T$ platí $a^n = a$.*

Důkaz Každý nenulový prvek tělesa T je kořenem polynomu $x^{n-1} - 1$, neboť je tvaru α^i pro primitivní prvek α tělesa T ($r(\alpha) = n-1$) - viz předchozí tvrzení. Tudíž každý (i nulový) prvek je kořenem polynomu $x^n - x$. ☒

6.27 Důsledek *Nechť T je konečné těleso charakteristiky p (aneb rozšíření tělesa $\mathbb{Z}_p$), a prvek $a \in T$. Pak vztah $a^p = a$ platí v tělese T právě, když $a \in \mathbb{Z}_p$.*

Důkaz Prvky $a \in \mathbb{Z}_p$ tento vztah splňují dle Fermatovy věty, tvoří tedy celkem p kořenů polynomu $x^p - x$. A více kořenů tento polynom stupně p v tělese T mít nemůže. ☒

6.28 Příklad Těleso $GF(8)$ sestrojené jako $T = \mathbb{Z}_2[x]/q(x)$, kde $q(x) = x^3 + x + 1$ je ireducibilní nad $\mathbb{Z}_2$, je těleso $T = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$.
$|T^*| = 7$, možné řády prvků $r \,|\, 7$, tedy kromě $a = 1$ (který má řád r(1) = 1) je každý nenulový prvek primitivním prvkem tělesa T. Použijeme prvek α a napíšeme každý nenulový prvek v T jako mocninu prvku α.

$$\alpha^1 = \alpha,\ \alpha^2 = \alpha^2,\ \alpha^3 = \alpha + 1,\ \alpha^4 = \alpha^2 + \alpha,\ \alpha^5 = \alpha^2 + \alpha + 1,\ \alpha^6 = \alpha^2 + 1,\ \alpha^7 = 1.$$

Tuto tabulku můžeme použít pro násobení v tělese T. Např.

$$(\alpha^2 + 1) \cdot (\alpha^2 + \alpha) = \alpha^6 \cdot \alpha^4 = \alpha^{10} = \alpha^7 \cdot \alpha^3 = 1 \cdot \alpha^3 = \alpha + 1$$

6.29 Třetí pohled na násobení v konečném tělese T o n prvcích: Nalezneme primitivní prvek β tělesa T a vytvoříme tabulku délky $(n-1)$, v níž je každý nenulový prvek napsán jako mocnina primitivního prvku β. Pak můžeme prvky násobit jako mocniny $\beta^k \cdot \beta^l = \beta^{k+l}$, přičemž v exponentu počítáme modulo $\mathrm{r}(\beta) = n-1$.

6.30 Příklad Těleso $GF(9)$ sestrojené jako $T = \mathbb{Z}_3[x]/q(x)$, kde $q(x) = x^2+1$ je ireducibilní nad $\mathbb{Z}_3$, je těleso komplexních čísel nad $\mathbb{Z}_3$, $T = \{a\,i + b,\ a, b \in \mathbb{Z}_3,\ i^2 = -1\}$.
$|T^*| = 8$, možné řády prvků $r \,|\, 8$. Přitom $i^4 = 1$, tedy $\mathrm{r}(i) = 4$, ale $(i+1)^4 \neq 1$, tedy $\mathrm{r}(i+1) = 8$ a $(i+1)$ je primitivním prvkem tělesa T.
Polynom $x^4 - 1$ má v tělese T všechny čtyři kořeny a jsou to prvky ± 1 a $\pm i$ tedy prvky podgrupy $\langle i \rangle$.

6.31 Poznámka Vždy lze setrojit těleso $GF(p^k)$ tak, aby kořen ireducibilního polynomu byl zároveň primitivním prvkem v tomto tělese. Aneb pro konstrukci tělesa $T = \mathbb{Z}_p[x]/q(x)$, lze zvolit ireducibilní polynom $q(x)$ stupně k tak, aby - napíšeme-li prvky tělesa T jako polynomy v proměnné z a počítáme dle pravidla $q(z) = 0$ - prvek z byl primitivním prvkem tělesa T.

6.32 Příklad Těleso $GF(9)$ sestrojené jako $T = \mathbb{Z}_3[x]/q(x)$, kde $q(x) = x^2 + x + 2$ je ireducibilní nad $\mathbb{Z}_3$, aneb těleso $T = \{a\,z + b,\ a, b \in \mathbb{Z}_3,\ z^2 = 2z + 1\}$.
$z^4 = (2z+1)^2 = z^2 + z + 1 = 2 \neq 1$, tedy $\mathrm{r}(z) = 8$ a z je primitivním prvkem tělesa T.

7 Polynomy nad $\mathbb{Z}_p$ a jejich kořeny v tělese T charakteristiky p

Těleso T charakteristiky p lze považovat za rozšíření tělesa $\mathbb{Z}_p$, tj. $\mathbb{Z}_p \subset T$. Pak každý polynom nad $\mathbb{Z}_p$ lze přirozeně považovat za polynom nad T a lze hledat jeho kořeny v tělese T. V předchozí kapitole jsme se dozvěděli, že každý prvek tělesa je kořenem polynomu $x^n - x$, kde $n = |T|$ (Fermatova věta), a že polynom $x^r - 1$ má v tělese r různých kořenů právě, když $r|n$, a jsou tvaru β^i, kde β je prvek řádu r. Nyní budeme zkoumat libovolné celočíselné polynomy s koeficienty v $\mathbb{Z}_p$ a jejich kořeny v tělese T.

7.1 Tvrzení *Nechť $q(x)$ je celočíselný polynom nad $\mathbb{Z}_p$ a nechť T je těleso charakteristiky p. Má-li polynom $q(x)$ kořen c v tělese T, pak má také kořen c^p v tělese T.*

Důkaz Označme $q(x) = a_n\, x^n + \ldots + a_1\, x + a_0$, kde $a_i \in \mathbb{Z}_p$. Víme, že c je kořen polynomu $q(x)$, tedy $q(c) = 0$. Potom $0 = 0^p = [q(c)]^p = a_n^p\, (c^n)^p + \ldots + a_1^p\, c^p + a_0^p$, neboť $\operatorname{char} T = p$. V důsledku Malé Fermatovy věty platí pro všechny prvky ze $\mathbb{Z}_p$, že $a_i^p = a_i$. Můžeme tedy dále upravit naši rovnost $0 = a_n\, (c^p)^n + \ldots + a_1\, c^p + a_0 = q(c^p)$ a dostáváme, že c^p je také kořen polynomu $q(x)$. ⊠

7.2 Důsledek *Nechť $q(x)$ je celočíselný polynom nad $\mathbb{Z}_p$ a nechť T je těleso charakteristiky p. Má-li polynom $q(x)$ kořen c v tělese T, pak má také kořeny $c^p, c^{(p^2)}, c^{(p^3)}, \ldots$ v tělese T.*

Tvorba kořenů se zastaví nejpozději po k krocích, kde $|T| = p^k$. Pro prvek c z tělesa T totiž platí $c^{(p^k)} = c$ podle Fermatovy věty.

7.3 Poznámka Podobnou situaci s kořeny v nadtělese známe u reálných polynomů a jejich komplexních kořenů. I zde je jistý vztah mezi kořeny, konkrétně má-li reálný polynom komplexní kořen $c = \alpha + \beta i$, pak musí mít i komplexně sdružený kořen $\bar{c} = \alpha - \beta i$.

7.4 Příklad Mějme těleso $GF(8)$ vyrobené takto: $T = \mathbb{Z}_2[x]/q(x)$, kde $q(x) = x^3 + x + 1$ je ireducibilní polynom nad $\mathbb{Z}_2$. Prvky tělesa označíme jako polynomy v proměnné α, tedy $T = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$. Polynom $q(x) = x^3 + x + 1$ je ireducibilní nad $\mathbb{Z}_2$, nemá tedy žádný kořen v tělese $\mathbb{Z}_2$.
V tělese T ale platí, že $q(\alpha) = \alpha^3 + \alpha + 1 = 0$, protože polynom $q(x)$ má nulový zbytek po dělení $q(x)$. Prvek α je tedy kořenem polynomu $q(x)$ v tělese T. Charakteristika tělesa $\operatorname{char} T = 2$, další kořeny polynomu $q(x)$ jsou α^2, $\alpha^4 = \alpha^2 + \alpha$ - můžeme to ověřit dosazením. Více kořenů není, neboť polynom stupně 3 může mít v tělese nejvýše tři kořeny - skutečně vyrábění dalších kořenů umocňováním na druhou se už zacyklí, $\alpha^8 = \alpha$, protože $|T| = 8$.

7.5 Tvrzení *Nechť $q(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$ stupně k. Pak v tělese $GF(p^k)$ tvaru $T = \mathbb{Z}_p[x]/q(x)$ má polynom $q(x)$ celkem k různých kořenů a polynom $q(x)$ se rozkládá na součin lineárních polynomů nad T.*

Důkaz $T = \{a_{k-1}\, z^{k-1} + \ldots + a_1\, z + a_0,\ a_i \in \mathbb{Z}_p, q(z) = 0\}$ Jedním kořenem polynomu $q(x)$ je prvek z a další kořeny vzniknou umocňováním na $\operatorname{char} T = p$, tedy z^p, z^{p^2}, …, $z^{p^{k-1}}$ jsou také kořeny polynomu $q(x)$. Zbývá dokázat, že jsou navzájem různé. To vyplývá z následujícího pojmu "minimální polynom". Pokud by se výroba kořenů zacyklila dříve než u $z^{(p^k)} = z$, pak by minimální polynom pro kořen z byl polynom nad $\mathbb{Z}_p$ stupně menšího než k a tento minimální polynom by dělil beze zbytku polynom $q(x)$, což by byl spor s ireducibilitou polynomu $q(x)$ nad $\mathbb{Z}_p$. ⊠

7.6 Definice Nechť T je konečné těleso charakteristiky p a prvek $c \in T$. *Minimální polynom nad $\mathbb{Z}_p$ pro prvek c* je nenulový celočíselný polynom nad $\mathbb{Z}_p$ co nejmenšího stupně, který má kořen c v tělese T. Označíme jej $m_c(x)$.

Takový polynom vždy existuje, neboť prvek $c \in T$ je dle Fermatovy věty kořenem celočíselného polynomu $x^{(p^k)} - x$, kde $p^k = |T|$. Mezi všemi nenulovými celočíselnými polynomy nad $\mathbb{Z}_p$ s kořenem $c \in T$ lze najít nějaký nejmenšího stupně. Zřejmě jeho konstantní násobek bude mít kořen c a bude téhož stupně - ukážeme, že minimální polynomy pro prvek c jsou navzájem asociované a jako $m_c(x)$ budeme značit ten, který má vedoucí koeficient roven 1 (monický minimální polynom pro prvek c).

7.7 Tvrzení *Nechť T je konečné těleso charakteristiky p a nechť c c^p, $c^{(p^2)}$, ..., $c^{(p^l)}$ jsou všechny různé prvky vzniklé umocňování prvku $c \in T$ na p-tou. Pak minimální polynom pro prvek c je polynom:*

$$m_c(x) = (x - c)(x - c^p) \cdot \ldots \cdot (x - c^{(p^l)})$$

Důkaz Každý celočíselný polynom nad $\mathbb{Z}_p$ musí mít s kořenem $c \in T$ také všechny tyto kořeny tvaru $c^{(p^i)}$. Jejich přidání je tedy nutné, dokážeme, že je i postačující. Označme a_i koeficienty výše vytvořeného polynomu $m_c(x)$. Spočítáme dvěma způsoby polynom $(m_c(x))^p$. Jelikož $\operatorname{char} T = p$, platí:

$$(m_c(x))^p = (\sum_{i=0}^{m} a_i x^i)^p = \sum_{i=0}^{m} a_i^p (x^p)^i$$

$$(m_c(x))^p = (x - c)^p (x - c^p)^p \cdot \ldots \cdot (x - c^{(p^l)})^p =$$

$$= (x^p - c^p)(x^p - c^{(p^2)}) \cdot \ldots \cdot (x^p - c^{(p^{l+1})}) = m_c(x^p) = \sum_{i=0}^{m} a_i (x^p)^i$$

Využili jsme toho, že $c^{p^{l+1}} = c$. Z rovnosti polynomů plyne, že $a_i^p = a_i$ pro všechna $0 \leq i \leq m$. To je možné jen, když všechna $a_i \in \mathbb{Z}_p$, polynom $m_c(x)$ je tedy celočíselný.

⊠

7.8 Tvrzení *Nechť $m_c(x)$ je minimální polynom nad $\mathbb{Z}_p$ pro prvek $c \in T$,* $\operatorname{char} T = p$. *Pak platí:*

1. *$m_c(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$*
2. *polynom $f(x)$ nad $\mathbb{Z}_p$ má kořen $c \in T$ právě, když $m_c(x) | f(x)$ nad $\mathbb{Z}_p$*

Důkaz 1) Kdyby $m_c(x) = a(x)b(x)$ byl netriviální rozklad nad $\mathbb{Z}_p$, pak by prvek c musel být kořenem polynomu $a(x)$ nebo $b(x)$ (neboť těleso nemá dělitele nuly), což by byl spor s tím, že $m_c(x)$ je celočíselný polynom nejmenšího stupně s kořenem c.
2) Celočíselný polynom $f(x)$ nad $\mathbb{Z}_p$ musí mít s kořenem $c \in T$ také všechny kořeny tvaru $c^{(p^i)}$, musí být tedy dělitelný všemi lineárními polynomy tvary $(x - c^{(p^i)})$. Proto je $f(x)$ dělitelný polynomem $m_c(x)$. ⊠

7.9 Důsledky

1. $f(x)$ je minimální polynom pro prvek c právě, když $f(x)$ je ireducibilní nad $\mathbb{Z}_p$ a $f(c) = 0$ v tělese T.
2. Monický $m_c(x)$ je určen jednoznačně.
3. $m_c(x) | (x^n - 1)$ právě, když $r(c) | n$.

Důkaz 1) $f(x)$ musí být dělitelný polynomem $m_c(x)$, ale protože $f(x)$ je ireducibilní nad $\mathbb{Z}_p$, tak $f(x) = a\, m_c(x)$ pro $a \in \mathbb{Z}_p$, tudíž $f(x)$ je také minimálním polynomem pro prvek c.
2) Minimální polynomy pro c se musí dělit navzájem (být asociované), monický je tedy jen jeden.
3) $m_c(x) | (x^n - 1)$ právě, když c je kořenem polynomu $x^n - 1$, aneb $c^n = 1$ v T. To nastane právě, když $r(c) | n$ - $r(c)$ je řád prvku c v grupě T^*. ⊠

7.10 Příklad Těleso $GF(8)$ sestrojené jako $T = \mathbb{Z}_2[x]/q(x)$, kde $q(x) = x^3 + x + 1$ je ireducibilní nad $\mathbb{Z}_2$, aneb $T = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$. Najdeme minimální polynomy pro všechny prvky.

Minimální polynom pro prvky ze $\mathbb{Z}_2$ jsou lineární: $m_0(x) = x$, $m_1(x) = x - 1$.
Minimální polynom pro kořen α je polynom $q(x) = x^3 + x + 1$, neboť $q(\alpha) = 0$ v tělese T a $q(x)$ je ireducibilní nad $\mathbb{Z}_2$. Tento polynom je také minimálním polynomem pro prvky α^2 a $\alpha^4 = \alpha^2 + \alpha$.
Najdeme minimální polynom pro kořen $\alpha + 1$ v tělese T. Další nutné kořeny jsou $(\alpha + 1)^2 = \alpha^2 + 1$, $(\alpha + 1)^4 = \alpha^2 + \alpha + 1$ a minimální polynom (pro tyto tři prvky) bude:

$$m_{\alpha+1}(x) = (x - (\alpha + 1))(x - (\alpha^2 + 1))(x - (\alpha^2 + \alpha + 1)) = x^3 + x^2 + 1$$

Můžeme to ověřit roznásobením, anebo odvodit následující úvahou: Víme, že má vyjít ireducibilní polynom stupně 3. Tyto polynomy jsou nad $\mathbb{Z}_2$ pouze dva, x^3+x+1 a x^3+x^2+1. První je roven polynomu $q(x) = m_\alpha(x)$ a nemá kořen $\alpha + 1$, takže $m_{\alpha+1}(x) = x^3 + x^2 + 1$.

Podle Fermatovy věty je každý prvek tělesa $GF(8)$ kořenem polynomu $x^8 - x$, tudíž minimální polynom každého prvku musí dělit polynom $x^8 - x$. A skutečně, rozložíme-li tento polynom na ireducibilní polynomy nad $\mathbb{Z}_2$, získáme $x^8 - x = x(x^7 - 1) = x(x - 1)(x^3 + x^2 + 1)(x^3 + x + 1)$.

Minimálních polynomů se využívá k důkazu faktu, že každé konečné komutativní těleso je Galoisovo.

7.11 Věta *Nechť T je konečné komutativní těleso charakteristiky p. Pak T je izomorfní s Galoisovým tělesem $\mathbb{Z}_p[x]/q(x)$, kde $q(x)$ je minimální polynom pro primitivní prvek tělesa T.*

Důkaz Hlavní myšlenka důkazu (detaily ponecháme čtenáři): Buď α primitivní prvek tělesa T a $m_\alpha(x)$ jeho minimální polynom, $\mathrm{st}(m_\alpha) = k$. Pak každý nenulový prvek tělesa T je tvaru $\beta = \alpha^i$. Podělíme-li se zbytkem polynom x^i polynomem $m_\alpha(x)$ v $\mathbb{Z}_p[x]$, dostaneme $x^i = q(x)m_\alpha(x) + t(x)$ a $st(t(x)) < k$. Můžeme tedy každý prvek zapsat ve tvaru polynomu v proměnné α stupně nejvýše $k - 1$, $\beta = \alpha^i = 0 + t(\alpha)$.
Přitom různé polynomy v proměnné α stupně nejvýše $k - 1$ určují různé prvky tělesa T: kdyby $t_1(\alpha) = t_2(\alpha)$, pak by $(t_1 - t_2)(\alpha) = 0$, ale α nemůže být kořenem žádného polynomu stupně menšího než k kromě nulového polynomu, tudíž $t_1(x) = t_2(x)$. Máme tedy vzájemně jednoznačné zobrazení mezi nenulovými prvky tělesa T a nenulovými polynomy nad $\mathbb{Z}_p$ stupně nejvýše $k - 1$. Prvku 0 přiřadíme nulový polynom.
Toto zobrazení je tělesovým izomorfismem mezi tělesem T a tělesem $\mathbb{Z}_p[x]/m_\alpha(x)$ - sčítání a násobení je respektováno, protože těleso T má charakteristiku p a protože je v něm $m_\alpha(\alpha) = 0$, 0 a 1 jsou respektovány zřejmě. ⊠

8 Kořeny cyklických kódů, BCH-kódy

Generující kořeny cyklických kódů

Nechť K je cyklický kód délky n nad $\mathbb{Z}_p$ s generujícím polynomem $g(z)$. Chceme najít rozšíření T tělesa $\mathbb{Z}_p$, tedy nějaké těleso $GF(p^k)$, ve kterém by měl polynom $g(x)$ stupně m celkem m různých kořenů. Pokud se mám to podaří, budou tyto kořeny společné všem kódovým polynomům a kód K jimi bude jednoznačně určen.

8.1 Příklad Uvažujme těleso $GF(8)$, $T = \mathbb{Z}_2[x]/x^3+x+1$, aneb $T = \{a\alpha^2+b\alpha+c,\, a,b,c \in \mathbb{Z}_2,\, \alpha^3 = \alpha+1\}$. Víme z předchozí kapitoly, že α je primitivní prvek tělesa T a že má minimální polynom $m_\alpha(x) = x^3+x+1$. Dále víme, že x^7-1 se nad $\mathbb{Z}_2$ rozkládá na ireducibilní polynomy takto: $x^7-1 = (x+1)(x^3+x^2+1)(x^3+x+1)$.

1) Lze tedy sestrojit cyklický kód K délky 7 nad $\mathbb{Z}_2$ s generujícím polynomem $g(z) = z^3+z+1$. Přitom $v(z) \in K$ právě, když $g(z) \,|\, v(z)$. Ale $g(z) = m_\alpha(z)$ a $v(z)$ je dělitelný minimálním polynomem $m_\alpha(z)$ s kořenem α právě, když $v(z)$ má také kořen α. Cyklický kód K je jednoznačně určen kořenem α: $K = \{v(z) \in \mathbb{Z}_2^{(7)}, v(\alpha) = 0\}$.

Kořene α lze využít ke kontrole - pokud $v(\alpha) \neq 0$ v tělese T, tak polynom $v(z)$ je chybný.
Z podmínky $v(\alpha) = 0$ odvodíme kontrolní matici kódu K. Slova převádíme na polynomy takto:

$$\bar{v} = (v_1, v_2, \ldots, v_6, v_7) \;\leftrightarrow\; v(z) = v_1 z^6 + v_2 z^5 + \ldots + v_6 z + v_7$$

Odtud

$$v(\alpha) = v_1\alpha^6 + v_2\alpha^5 + \ldots + v_6\alpha + v_7 = (\alpha^6\, \alpha^5\, \ldots\, \alpha\, 1)\cdot \bar{v}^T = 0$$

a kontrolní matice nad tělesem T pro kód K je $\mathbb{H} = (\alpha^6\, \alpha^5\, \ldots\, \alpha\, 1)$. Rozepíšeme-li mocniny prvku α na polynomy stupně nejvýše 2 (prvky tělesa T), získáme homogenní soustavu nad $\mathbb{Z}_2$ pro kódová slova:

$$v(\alpha) = v_1(\alpha^2+1) + v_2(\alpha^2+\alpha+1) + \ldots + v_6\alpha + v_7 = 0$$

právě, když (první rovnice následující soustavy je pro koeficienty u α^2, druhá u α, třetí u 1)

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \cdot \bar{v}^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Matice této soustavy je kontrolní maticí $\mathbb{H}$ nad $\mathbb{Z}_2$ pro kód K.
Sloupec $\alpha^i = a\alpha^2 + b\alpha + c$ v matici $\mathbb{H}$ nad T odpovídá sloupci $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ v matici $\mathbb{H}$ nad $\mathbb{Z}_2$.

Všimněme si, že kontrolní matice $\mathbb{H}$ má za sloupce všechny nenulové trojice nad $\mathbb{Z}_2$ (protože α byl primitivní prvek a vygeneroval všechny nenulové prvky tělesa T). Náš kód K je tedy cyklický Hammingův kód se třemi kontrolními znaky.
Tudíž opravuje 1 chybu a opravování lze také dělat pomocí kořene α. V případě jedné chyby je $w(z) = v(z) + a\, z^i = v(z) + z^i$ (neboť $a \in \mathbb{Z}_2$), pro nějaký $v(z) \in K$. Pak $w(\alpha) =$ "polynom v α stupně nejvýše 2"$= 0 + \alpha^i$, přičemž mocnina primitivního prvku α^i je určena jednoznačně, tudíž chyba je v i-té mocnině.

2) Analogicky lze sestrojit cyklický kód K' délky 7 nad $\mathbb{Z}_2$ s generujícím polynomem $g(z) = (z+1)(z^3+z+1)$. Přitom $v(z) \in K'$ právě, když $g(z) \,|\, v(z)$. Ale $g(z) = m_1(z)m_\alpha(z)$ a $v(z)$ je dělitelný oběma minimálními (a tudíž ireducibilními) polynomy $m_1(z)$ i $m_\alpha(z)$ právě, když $v(z)$ má kořeny α a 1 v tělese T. Cyklický kód K je jednoznačně určen kořeny α, 1: $K = \{v(z) \in \mathbb{Z}_2^7, v(\alpha) = 0$ a $v(1) = 0\}$.
Kontrolní matice pro kód K' bude

$$\mathbb{H} = \begin{pmatrix} \alpha^6 & \alpha^5 & \ldots & \alpha & 1 \\ 1^6 & 1^5 & \ldots & 1 & 1 \end{pmatrix} \text{ nad } T \;\leftrightarrow\; \mathbb{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ nad } \mathbb{Z}_2\,.$$

8.2 Definice *Generující kořeny* cyklického kódu K délky n nad $\mathbb{Z}_p$ jsou takové prvky $c_1, c_2, \ldots, c_m$ nějakého tělesa $GF(p^k)$, že pro každý $v(z) \in \mathbb{Z}_p^{(n)}$ je $v(z) \in K$ právě, když $v(z)$ má kořeny $c_1, c_2, \ldots, c_m$ v tělese $GF(p^k)$.

8.3 Poznámka Generující kořeny nejsou určeny jednoznačně, protože kódové polynomy jsou celočíselné polynomy nad $\mathbb{Z}_p$ a mají v tělese charakteristiky p s kořenem c automaticky také kořeny c^p, $c^{(p^2)}$, atd. Například kód K délky 7 nad $\mathbb{Z}_2$ s generujícím polynomem $g(z) = z^3+z+1$ z prvního příkladu má v tělese $T = \mathbb{Z}_2[x]/x^3+x+1$ generující kořen α, ale také má generující kořeny α, α^2 a $\alpha^4 = \alpha^2 + \alpha$. Stejně tak je generujícím kořenem kódu K prvek α^2.

8.4 Tvrzení *Cyklický kód K délky n nad $\mathbb{Z}_p$ má v tělese $GF(p^k)$ generující kořeny právě, když má jeho generující polynom $g(z)$ v tělese T tolik navzájem různých kořenů, kolik je jeho stupeň.*

Důkaz Nechť $g(z)$ je stupně m a má v tělese T celkem m různých kořenů $c_1, c_2, \ldots, c_m$. Kódové polynomy jsou násobky generujícího polynomu, $v(z) \in K$ právě, když $v(z) = a(z)g(z)$. Tudíž $c_1, c_2, \ldots, c_m$ jsou též kořeny každého kódového polynomu. Naopak, protože kořeny jsou různé, tak každý polynom s kořeny $c_1, c_2, \ldots, c_m$ je dělitelný $\prod_{i=1}^{m}(z - c_i)$, ale polynom $g(z) = \prod_{i=1}^{m}(z - c_i)$, neboť $\mathrm{st}(g) = m$ a $c_1, c_2, \ldots, c_m$ jsou jeho kořeny (můžeme předpokládat, že generující polynom je monický). Takže každý polynom s kořeny $c_1, c_2, \ldots, c_m$ je kódovým polynomem.
Má-li $g(z)$ v tělese T méně než m různých kořenů, pak existují polynomy, které tyto kořeny mají také a přesto nejsou dělitelné polynomem $g(z)$, aneb nejsou to kódové polynomy. ⊠

8.5 Příklad Polynom $x^5 - 1$ se nad $\mathbb{Z}_5$ rozkládá na ireducibilní polynomy takto: $x^5 - 1 = (x - 1)^5$. Lze tedy sestrojit cyklický kód K délky 5 nad $\mathbb{Z}_5$ s generujícím polynomem $g(z) = (z - 1)^2$. Každý kódový polynom je dělitelný polynomem $g(z)$, má tedy kořen 1 v $\mathbb{Z}_5$. Ale ne každý polynom s kořenem 1 je kódový, neboť kořen 1 může být jen jednonásobný. Vlastnost $v(1) = 0$ necharakterizuje jednoznačně kód K.

8.6 Cyklický kód K délky n nad $\mathbb{Z}_p$ je svými generujícími kořeny v tělese $GF(p^k)$ (označme je T) jednoznačně určen. Z generujících kořenů spočteme generující polynom i kontrolní matici.

Generující polynom je nenulový kódový polynom nejmenšího stupně, aneb nenulový polynom nad $\mathbb{Z}_p$ nejmenšího stupně s danými kořeny v tělese. Je-li generujícím kořenem jeden prvek c, jedná se o minimální polynom pro tento prvek, tj. $g(z) = m_c(z)$. Jsou-li generujícími kořeny prvky $c_1, c_2, \ldots, c_m$, jedná se o součin minimálních polynomů pro ty prvky, které mají různé minimální polynomy (aneb které splňují $c_i \neq c_j^{(p^l)}$):

$$g(z) = \mathrm{lcm}(m_{c_1}(z), \ldots, m_{c_l}(z)) = \prod_{\text{přes různé polynomy}} m_{c_i}(z)$$

Kontrolní matice cyklického kódu K délky n s generujícím kořenem c je odvozena ze vztahu $v(c) = 0$, což je vlastně homogenní "soustava", kterou musí splňovat kódové polynomy. Matice této soustavy je $\mathbb{H} = \begin{pmatrix} c^{n-1} & c^{n-2} & \ldots & c & 1 \end{pmatrix}$ nad tělesem T. Nahradíme-li každé c^i = "polynom stupně nejvýše k v tělese T" sloupcem jeho koeficientů, získáme matici $\mathbb{H}$ o k řádcích nad $\mathbb{Z}_p$. Jsou-li v této matici některé řádky lineární kombinací ostatních, můžeme je vyškrtnout (a získáme matici pro ekvivalentní homogenní soustavu rovnic).
Kontrolní matice kódu K délky n s generujícími kořeny $c_1, c_2, \ldots, c_m$ se získá analogicky z matice

$$\mathbb{H} = \begin{pmatrix} c_1^{n-1} & c_1^{n-2} & \ldots & c_1 & 1 \\ c_2^{n-1} & c_2^{n-2} & \ldots & c_2 & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ c_m^{n-1} & c_m^{n-2} & \ldots & c_m & 1 \end{pmatrix} \text{ nad } T\,.$$

Opravování jedné chyby: Cyklický kód nad $\mathbb{Z}_p$ s jedním generujícím kořenem pro $p > 2$ většinou neopravuje jednu chybu. V případě jedné chyby je $w(z) = v(z) + a\,z^i$ pro $v(z) \in K$. Například nad $\mathbb{Z}_3$ mohou být dvě možnosti, jak vyjádřit "syndrom" ve tvaru $a\,c^i$, neboť může být $w(c) = 1\,c^i$ ale taky $w(c) = 2\,c^j$. Nevíme tedy, zda chybový polynom je $e(z) = 1\,z^i$ nebo $e(z) = 2\,z^j$, a neumíme chybu opravit.
Cyklický kód nad $\mathbb{Z}_p$ s více generujícími kořeny jednu chybu už opravovat může a lze to udělat pomocí kořenů. Vyjádříme syndrom pro každý kořen c_k všemi možnostmi jako $w(c_k) = a\,(c_k)^i$ (pro různá $a \in \mathbb{Z}_p$ a různá $0 \leq i \leq n-1$) a je-li pouze jediná možnost společná všem kořenům, pak tato možnost určuje chybový polynom.

8.7 Otázka č.1 Máme těleso T o p^k prvcích a v něm vybereme prvky $c_1, c_2, \ldots, c_m$. Chceme, aby tyto prvky byly generujícími kořeny cyklického kódu nad $\mathbb{Z}_p$. Pro jakou délku n kódových slov je to možné?

Víme, že generující polynom cyklického kódu délky n musí dělit $x^n - 1$ v $\mathbb{Z}_p[x]$. $g(z) = \mathrm{lcm}(m_{c_1}(z), \ldots, m_{c_l}(z))$, takže každý minimální polynom $m_{c_i}(x)$ musí dělit $x^n - 1$. Ale $m_{c_i}(x) \mid x^n - 1$ právě, když c_i je kořen $x^n - 1$, aneb když $c_i^n = 1$. Dostáváme podmínku, že řád každého kořene c_i musí dělit n. Délka cyklického kódu s generujícími kořeny $c_1, c_2, \ldots, c_m$ je $n = l \cdot \mathrm{lcm}(\mathrm{r}(c_1), \ldots, \mathrm{r}(c_m))$ pro libovolné $l \in \mathbb{N}$.

8.8 Příklad Je dáno těleso komplexních čísel nad $\mathbb{Z}_3$, $T = \mathbb{Z}_3[x]/x^2 + 1 = \{ai + b, a, b \in \mathbb{Z}_3,\ i^2 = -1\}$.
a) Cyklický kód s generujícím kořenem i v tělese T má nejmenší možnou délku $n = \mathrm{r}(i) = 4$. Jeho generující polynom je $g(z) = m_i(z) = z^2 + 1$. Jeho kontrolní matice je $\mathbb{H} = (i^3\ i^2\ i\ 1)$ nad tělesem T, což odpovídá matici $\mathbb{H} = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix}$ nad $\mathbb{Z}_3$.
b) Cyklický kód s generujícími kořeny i a $i+1$ v tělese T má nejmenší délku $n = \mathrm{lcm}(\mathrm{r}(i), \mathrm{r}(i+1)) = 8$. Jeho generující polynom je $g(z) = m_i(z)m_{i+1}(z) = (z^2+1)(z^2+z+2) = z^4 + z^3 + z + 2$. Jeho kontrolní matice je

$$\mathbb{H} = \begin{pmatrix} (i+1)^7 & (i+1)^6 & (i+1)^5 & \ldots & (i+1) & 1 \\ i^7 & i^6 & i^5 & \ldots & i & 1 \end{pmatrix} \longleftrightarrow \mathbb{H} = \begin{pmatrix} 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \\ 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 \end{pmatrix}.$$

Opravíme ještě jednu chybu ve slově $\bar{w} = (1\ 1\ 0\ 0\ 0\ 0\ 2\ 1)$ pomocí dosazování kořenů.
$w(i) = i^7 + i^6 + 2i + 1 = 2i + 2 + 2i + 1 = i = a\ i^j = 1\ i^1 = 1\ i^5 = 2\ i^3 = 2\ i^7$
$w(i+1) = (i+1)^7 + (i+1)^6 + 2(i+1) + 1 = (i+2) + i + 2(i+1) + 1 = i + 2 = a\ (i+1)^j = 1\ (i+1)^7 = 2\ (i+1)^3$
Chybový polynom je určen jednoznačně, jediná možnost odpovídající oběma kořenům je $e(z) = 2\ z^3$. Opravíme $v(z) = w(z) - e(z)$, tedy $\bar{v} = (1\ 1\ 0\ 0\ 1\ 0\ 2\ 1)$.

8.9 Otázka č. 2. Máme cyklický kód K délky n nad $\mathbb{Z}_p$. V jakém tělese T lze najít jeho generující kořeny? Musí takové těleso vždy existovat?

Hledáme tedy rozšíření T tělesa $\mathbb{Z}_p$, ve kterém by měl generující polynom $g(x)$ stupně m celkem m různých kořenů. Víme, že generující polynom $g(x)$ je dělitelem polynomu $x^n - 1$ nad $\mathbb{Z}_p$. Pokusíme se tedy najít těleso T charakteristiky p, tedy nějaké $GF(p^k)$, nad kterým by se polynom $x^n - 1$ rozkládal na kořenové činitele (s jednonásobnými kořeny).

V tělese T o p^k prvcích má polynom $x^n - 1$ celkem n různých kořenů právě, když je n dělitelem počtu prvků cyklické grupy T^*, tedy když $n \mid p^k - 1$. Kořeny jsou pak všechny prvky n-prvkové podgrupy generované prvkem β řádu n a mají tvar β^i pro $1 \leq i \leq n$. Hledáme tedy k tak, aby $n \mid p^k - 1$. Přitom

$$n \mid p^k - 1 \qquad \text{iff} \qquad p^k - 1 = 0 \ \text{ v } \ \mathbb{Z}_n \qquad \text{iff} \qquad p^k = 1 \ \text{ v } \ \mathbb{Z}_n$$

Takové k lze najít jenom, když p není dělitelem čísla n. Z rovnosti $p^k = 1$ lze totiž spočítat inverzní prvek k prvku p, konkrétně $p^{-1} = p^{k-1}$ v $\mathbb{Z}_n$. Víme, že v $\mathbb{Z}_n$ jsou invertibilní pouze prvky nesoudělné s n, takže p musí být nesoudělné s n, což pro prvočíslo p nastane právě, když $p \nmid n$.

Dostáváme podmínku $p \nmid n$, bez níž bychom nemohli vyřešit naši úlohu - nemohli bychom najít těleso těleso T o p^k prvcích, v němž má polynom $x^n - 1$ celkem n různých kořenů. Podíváme-li se na to z druhé strany, tak pro $n = mp$ lze v tělese T charakteristiky p rozložit polynom $x^n - 1 = x^{mp} - 1 = (x^m - 1)^p$. Tudíž všechny jeho kořeny budou aspoň p-násobné a nebude n různých kořenů.

Pokud $p \nmid n$, pak naši úlohu skutečně vyřešíme. Euler-Fermatova věta tvrdí:

$$\text{Když } \ p \nmid n, \ \text{ pak } \ p^{\varphi(n)} = 1 \ \text{ v } \ \mathbb{Z}_n.$$

Můžeme tedy volit $k = \varphi(n)$, pak v tělese $GF(p^{\varphi(n)})$ bude mít polynom $x^n - 1$ celkem n různých kořenů.
Mohou ale existovat i menší tělesa, která řeší naši úlohu. To nejmenší k, které splňuje $p^k = 1$ v grupě invertibilních prvků $\mathbb{Z}_n^*$, je vlastně řád prvku p v této grupě, $k = \mathrm{r}(p)$ v $\mathbb{Z}_n^*$. Dokonce víme:

$$p^k = 1 \ \text{ v } \ \mathbb{Z}_n^* \quad \text{právě, když} \quad \mathrm{r}(p) \mid k$$

Těles $GF(p^k)$, v nichž má polynom $x^n - 1$ celkem n různých kořenů, je tedy nekonečně mnoho (za předpokladu, že $p \nmid n$).

Shrňme naše úvahy do následujícího tvrzení:

8.10 Tvrzení *Nechť K je cyklický kód délky n nad $\mathbb{Z}_p$ s generujícím polynomem $g(z)$ stupně m a nechť $p \nmid n$. Položme $k = \varphi(n)$ (anebo $k = \mathrm{r}(p)$ v grupě $\mathbb{Z}_n^*$). Pak v tělese $GF(p^k)$ má generující polynom $g(z)$ právě m různých kořenů tvaru $\beta^{i_1}, \beta^{i_2}, \ldots, \beta^{i_m}$ pro nějaký prvek β řádu n v tělese $GF(p^k)$ (aneb nalezneme je mezi kořeny polynomu $x^n - 1$). Tyto kořeny jsou generujícími kořeny cyklického kódu K.*

8.11 Příklad Cyklický kód K délky 4 nad $\mathbb{Z}_7$ má generující polynom $g(z) = z^2 + 1$. Jeho generující kořeny budeme hledat v tělese $GF(7^k)$, kde $k = \varphi(4) = 2$. Zkonstruujeme těleso $GF(49)$, $T = \mathbb{Z}_7[x]/q(x)$, kde $q(x)$ bude ireducibilní nad $\mathbb{Z}_7$ stupně 2. Najdeme jeho primitivní prvek (označme ho α, aneb $\mathrm{r}(\alpha) = 48$) a dopočteme prvek řádu $n = 4$ (označme ho $\beta = \alpha^{12}$). Generující kořeny kódu K budou dva z prvků β, β^2, β^3 a $\beta^4 = 1$, určíme je dosazováním.

BCH-kódy

Pokud budeme volit kořeny "šikovně", můžeme zaručit opravování předem daného množství chyb. Následující konstrukci vymysleli pánové Bose a Ray-Chaudhuri a nezávisle na nich pan Hocquenghem.

8.12 Definice *BCH-kód* délky n nad $\mathbb{Z}_p$ ($p \nmid n$) *s plánovanou vzdáleností* d ($d \leq n$) je cyklický kód s generujícími kořeny $\beta, \beta^2, \beta^3, \ldots, \beta^{d-1}$, kde β je prvek řádu n v nějakém tělese $GF(p^k)$.

8.13 Tvrzení *BCH-kód K délky n nad $\mathbb{Z}_p$ s plánovanou vzdáleností d má skutečnou Hammingovu vzdálenost kódu $d_H(K) \geq d$.*

Tudíž BCH-kód s plánovanou vzdáleností d objevuje $(d-1)$ chyb a opravuje $[\frac{d-1}{2}]$ chyb.

8.14 Poznámka Pro vytvoření BCH-kódu nad $\mathbb{Z}_p$ s plánovanou vzdáleností d není vždy nutné vyžadovat všechny kořeny $\beta, \beta^2, \ldots, \beta^{d-1}$. Kódové polynomy jsou polynomy nad $\mathbb{Z}_p$ a tudíž musí mít v tělese charakteristiky p s kořenem c, také kořeny c^p, $c^{(p^2)}$, atd. Speciálně pro BCH-kódy nad $\mathbb{Z}_2$ s (lichou) plánovanou vzdáleností d stačí požadovat kořeny $\beta, \beta^3, \beta^5, \ldots, \beta^{d-2}$, neboť potom prvky $\beta^2, \beta^4, \beta^6, \ldots, \beta^{d-1}$ budou také kořeny daného kódu.

8.15 BCH-kódy nad $\mathbb{Z}_p$ délky $n = p^k - 1$: Má-li BCH-kód nad $\mathbb{Z}_p$ délku $n = p^k - 1$, pak je kořen β primitivním prvkem v tělese $GF(p^k)$ (kde $p^k = n + 1$). Vždy lze zvolit ireducibilní polynom $q(x)$ stupně k tak, aby kořen α tohoto polynomu byl primitivním prvkem tělesa $T = \mathbb{Z}_p[x]/q(x)$, jehož prvky zapisujeme jako polynomy stupně nejvýše $k-1$ v proměnné α. Provedeme-li takovouto konstrukci tělesa $GF(p^k)$, pak volíme za kořen $\beta = \alpha$.

BCH-kódy nad $\mathbb{Z}_p$ délky $n = p^k - 1$ s jediným generujícím kořenem α v tomto tělese budou mít generující polynom $g(z) = m_\alpha(z) = q(z)$ a jejich kontrolní matice $\mathbb{H} = \begin{pmatrix} \alpha^{n-1} & \alpha^{n-2} & \ldots & \alpha & 1 \end{pmatrix}$ nad T obsahuje všechny nenulové prvky tělesa T. Tudíž kontrolní matice $\mathbb{H}$ nad $\mathbb{Z}_p$ má ve sloupcích všechny nenulové k-tice nad $\mathbb{Z}_p$. Každé dva sloupce matice $\mathbb{H}$ jsou lineárně nezávislé právě, když pracujeme nad $\mathbb{Z}_2$ (neboť nad $\mathbb{Z}_p$, $p > 2$, jsou v $\mathbb{H}$ sloupce S a $2S$, které jsou různé, ale lineárně závislé). Tedy BCH-kódy nad $\mathbb{Z}_2$ opravují jednu chybu a mají Hammingovu vzdálenost $d_H(K) = 3$. Ale to není překvapující, neboť kódové polynomy nad $\mathbb{Z}_2$ mají v tělese charakteristiky 2 s kořenem α také kořen α^2 (a α^4, atd.), tedy dvě po sobě jdoucí mocniny prvku α, a jsou to vlastně BCH-kódy s plánovanou vzdáleností $d = 3$. BCH-kód nad $\mathbb{Z}_2$ délky $n = 2^k - 1$ s jedním kořenem je tudíž **cyklický Hammnigův kód** o k kontrolních znacích.

BCH-kódy nad $\mathbb{Z}_2$ délky $n = p^k - 1$ s generujícími kořeny $\alpha, \alpha^3, \alpha^5, \ldots, \alpha^{2t-1}$ ve výše zkonstruovaném tělese, jsou podprostory Hammingových kódů. Opravují t chyb a mají velmi dobrý informační poměr ("relativně malou" redundanci). Jsou pro ně také vypracovány metody, jak opravovat vícenásobné chyby pomocí kořenů.

8.16 Příklad Cyklický kód délky $n = 7$ opravující dvě chyby má Hammingovu vzdálenost $d_H(K) = 5$. Vyrobíme BCH-kód s plánovanou vzdáleností $d = 5$. Použijeme těleso $GF(2^3) = GF(8)$, například těleso $T = \mathbb{Z}_2[x]/x^3 + x + 1 = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$, které má primitivní prvek α. Za kořeny volíme prvky α a $\alpha^3 = \alpha + 1$.

Kontrolní matice nad T, resp. nad $\mathbb{Z}_2$ je

$$\mathbb{H} = \begin{pmatrix} \alpha^6 & \alpha^5 & \dots & \alpha & 1 \\ (\alpha+1)^6 & (\alpha+1)^5 & \dots & (\alpha+1) & 1 \end{pmatrix} \longleftrightarrow \mathbb{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Generující polynom je (viz předchozí kapitola)

$$g(z) = m_\alpha(z) m_{\alpha+1}(z) = (z^3 + z + 1)(z^3 + z^2 + 1) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1.$$

Jde o opakovací kód délky 7 a jeho skutečná Hammingova vzdálenost je $d_H(K) = 7$, tedy větší než plánovaná vzdálenost $d = 5$.

8.17 BCH-kódy nad $\mathbb{Z}_p$ délky $n \neq p^k - 1$: Má-li BCH-kód nad $\mathbb{Z}_p$ délku $n \neq p^k - 1$, pak je β prvkem řádu n v tělese $GF(p^k)$, kde volíme $k = \varphi(n)$ (anebo $k = \mathrm{r}(p)$ v grupě $\mathbb{Z}_n^*$). Tato volba zafunguje kdykoli $p \nmid n$ (viz odpověď na otázku č.2).

8.18 Příklad BCH-kód délky $n = 9$ nad $\mathbb{Z}_2$ s plánovanou vzdáleností $d = 3$ bude mít za kořen prvek β řádu $\mathrm{r}(\beta) = 9$ v tělese $GF(2^{\varphi(9)}) = GF(2^6) = GF(64)$. Menší těleso $GF(2^k)$ obsahující prvek řádu 9 nenajdeme, protože $\mathrm{r}(2) = 6$ v grupě $\mathbb{Z}_9^*$. Toto těleso sestrojíme jako $\mathbb{Z}_2[x]/q(x)$, kde $q(x)$ bude polynom šestého stupně ireducibilní nad $\mathbb{Z}_2$. Prvky tělesa budou polynomy nejvýše pátého stupně zapsané v proměnné α a přepisovací pravidla budou dána vztahem $q(\alpha) = 0$. V tělese najdeme primitivní prvek, při šikovné volbě ireducibilního polynomu $q(x)$ bude primitivním prvkem přímo prvek α a $\mathrm{r}(\alpha) = 63$. Potom generujícím kořenem našeho BCH-kódu bude prvek $\beta = \alpha^7$, neboť $\mathrm{r}(\beta) = \mathrm{r}(\alpha^7) = 9$.