Kapitola 4

Tělesa

Dosud jsme se zabývali pouze soustavami lineárních rovnic s reálnými koeficienty. Všechna čísla byla reálná, vektory měly reálné souřadnice, matice měly reálné prvky. Také řešení soustav lineárních rovnic jsme hledali mezi reálnými vektory. Reálná čísla jsou pouze jedním z mnoha číselných oborů. Navíc mají jednu velkou nevýhodu – nelze s nimi počítat exaktně. Iracionální čísla nelze vyjádřit jinak než pomocí nekonečného desetinného rozvoje a každý výpočetní systém je proto musí zaokrouhlovat. A zaokrouhlování, jak už víme, s sebou přináší problém zaokrouhlovacích chyb.

Pokud počítáme s racionálními čísly a vyjadřujeme je jako zlomky, tak se problému zaokrouhlovacích chyb vyhneme. Můžeme počítat v exaktní aritmetice. Když si projdeme texty dosavadních přednášek, tak zjistíme, že jsme ve skutečnosti nikde nevyužívali předpoklad, že počítáme právě s reálnými čísly. Veškerý dosavadní text zůstane v platnosti pokud se omezíme pouze na počítání s racionálními čísly. Gaussova eliminace a zpětné dosazování bude fungovat zcela stejně, všechna řešení soustavy lineárních rovnic s racionálními koeficienty budou opět racionální čísla, resp. vektory s racionálními souřadnicemi. Má-li nějaká regulární matice pouze racionální prvky, tak také matice k ní inverzní bude tvořena pouze racionálními čísly. Dosud jsme používali pouze operace sčítání/odčítání a násobení/dělení. Množina všech racionálních čísel je na tyto operace *uzavřená*, součin nebo rozdíl dvou racionálních čísel je opět racionální číslo a stejně tak součin nebo podíl racionálních čísel je také racionální číslo. Nikde jsme dosud nepoužívali odmocňování, kde by nám racionální čísla nestačila. Druhá odmocnina ze 2 totiž racionální není.

Podobně také můžeme místo v oboru reálných čísel počítat ve větším oboru komplexních čísel a všechy dosud získané poznatky zůstanou v plat-

nosti. LU faktorizace regulární matice s komplexními prvky bude tvořena dvěma trojúhelníkovými maticemi s komplexními prvky, atd. V případě komplexních čísel by nám nevadilo ani odmocňování.

Ve skutečnosti vůbec nejde o to, s jakými čísly počítáme, ale o to, jaké algebraické vlastnosti toto počítání, tj. sčítání a násobení, má. Veškeré dosud získané poznatky závisejí na několika vlastnostech těchto operací, které jsou obsahem následující důležité definice.

Definice 4.1 *Předpokládáme, že* $\mathbf{T}$ *je množina, na které jsou definované dvě operace – sčítání a násobení. Pokud tyto dvě operace splňují následující podmínky (axiomy), říkáme že množina* $\mathbf{T}$ *spolu s těmito operacemi tvoří* těleso. *Jsou to podmínky*

(A0) *součet* $a + b \in \mathbf{T}$ *pro libovolné* $a, b \in \mathbf{T}$,

(A1) *platí* $(a + b) + c = a + (b + c)$ *pro libovolné* $a, b, c \in \mathbf{T}$,

(A2) $a + b = b + a$ *pro libovolné dva prvky* $a, b \in \mathbf{T}$,

(A3) *existuje prvek* $0 \in \mathbf{T}$ *takový, že* $0 + a = a$ *pro každé* $a \in \mathbf{T}$,

(A4) *ke každému prvku* $a \in \mathbf{T}$ *existuje prvek* $-a \in \mathbf{T}$, *pro který platí, že* $(-a) + a = 0$.

To jsou všechny axiomy pro sčítání. Axiom (A0) říká, že množina $\mathbf{T}$ *je* uzavřená *na sčítání. Axiom (A1) je* asociativita *sčítání, axiom (A2) je* komutativita *sčítání. Axiomu (A3) říkáme existence* nulového prvku *nebo také* neutrálního prvku *vzhledem ke sčítání a axiomu (A4) pak existence* opačného prvku *vzhledem ke sčítání.*

Následují axiomy pro násobení:

(M0) *součin* $ab \in \mathbf{T}$ *pro libovolné* $a, b \in \mathbf{T}$,

(M1) *platí* $(ab)c = a(bc)$ *pro libovolné* $a, b, c \in \mathbf{T}$,

(M2) $ab = ba$ *pro libovolné dva prvky* $a, b \in \mathbf{T}$,

(M3) *existuje prvek* $1 \in \mathbf{T}$ *takový, že* $1a = a$ *pro každé* $a \in \mathbf{T}$,

(M4) *ke každému prvku* $0 \neq a \in \mathbf{T}$ *existuje prvek* $a^{-1} \in \mathbf{T}$, *pro který platí* $a^{-1}a = 1$.

Axiom (M0) vyjadřujeme slovy, že množina $\mathbf{T}$ *je* uzavřená *vzhledem k násobení, axiomy (M1) a (M2) říkají, že násobení je* asociativní *a* komutativní. *Axiom (M3) je existence* jednotkového prvku *nebo také* neutrálního prvku *vzhledem k násobení a axiom (M4) je axiom existence* inverzního prvku *vzhledem k násobení.*

Obě operace pak spojuje axiom distributivity

(D) *platí* $a(b+c) = ab + ac$ *pro libovolné tři prvky* $a, b, c \in \mathbf{T}$.

A nakonec axiom netriviality

(N) $0 \neq 1$.

V axiomu distributivity jsme použili obvyklou konvenci, že násobení má přednost před sčítáním, pokud pomocí závorek neurčíme jiné pořadí provádění operací. Axiom netriviality říká, že každé těleso má aspoň dva prvky.

Všechny dosavadní poznatky o maticích a řešení soustav lineárních rovnic platí v libovolném tělese $\mathbf{T}$. Soustavou lineárních rovnic v tělese $\mathbf{T}$ rozumíme soustavu

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2, \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m, \end{aligned}$$

kde jsou všechny koeficienty $a_{ij}, b_k \in \mathbf{T}$. Z axiomů tělesa a jejich bezprostředních důsledků pak vyplývá, že Gaussova eliminace a zpětná substituce vedou k řešením této soustavy, která všechna opět leží v tělese $\mathbf{T}$.

Podobně matice s prvky z tělesa $\mathbf{T}$ je matice $\mathbf{A} = (a_{ij})$, kde $a_{ij} \in \mathbf{T}$. Elementární řádkové úpravy matice s prvky z libovolného tělesa $\mathbf{T}$ můžeme provádět beze změny. Proto zůstává v platnosti i definice hodnosti matice. Je-li $\mathbf{A}$ regulární matice, pak Gaussova-Jordanova eliminace vede k inverzní matici $\mathbf{A}^{-1}$, která má také prvky z tělesa $\mathbf{T}$. Podobně zůstávají v platnosti i všechny ostatní vlastnosti matic. Stačí pouze vždy na začátku říct, v jakém tělese leží prvky matic, se kterými počítáme.

Tvrzení 4.2 *V každém tělese* $\mathbf{T}$ *platí*

1. *nulový prvek je určený jednoznačně,*
2. *opačný prvek* $-a$ *je prvkem* $a \in \mathbf{T}$ *určený jednoznačně,*

3. *jednotkový prvek je určený jednoznačně,*
4. *prvek a^{-1} inverzní k prvku $0 \neq a \in \mathbf{T}$, je prvkem a určený jednoznačně,*
5. *$0a = 0$ pro libolný prvek $a \in \mathbf{T}$,*
6. *je-li $ab = 0$, pak buď $a = 0$ nebo $b = 0$,*
7. *$(-1)a = -a$ pro každý prvek $a \in \mathbf{T}$,*
8. *rovnice $ax = b$, $a \neq 0$, má vždy právě jedno řešení,*
9. *rovnice $c + x = d$ má vždy právě jedno řešení,*
10. *z rovnosti $ab = ac$ a předpokladu $a \neq 0$, vyplývá $b = c$,*
11. *z rovnosti $a + b = a + c$ plyne $b = c$,*
12. *$(-a)(-b) = ab$ pro každé dva prvky $a, b \in \mathbf{T}$.*

Důkaz. Všechny důkazy jsou jednoduché, je pouze třeba v každém kroku ukázat, který z axiomů tělesa, případně z již dokázaných důsledků, používáme.

1. Jsou-li 0 a $\overline{0}$ prvky neutrální vzhledem ke sčítání, pak platí

$$\overline{0} = 0 + \overline{0} = \overline{0} + 0 = 0.$$

První rovnost plyne z axiomu (A3), protože 0 je neutrální vzhledem ke sčítání. Druhá rovnost plyne z (A2) a třetí z (A3), protože také prvek $\overline{0}$ je neutrální vzhledem ke sčítání.

2. Je-li $b \in \mathbf{T}$ také prvek opačný k prvku a, pak platí

$$b = 0 + b = ((-a) + a) + b = (-a) + (a + b) = (-a) + 0 = -a.$$

První rovnost plyne z (A3), druhá z (A4), třetí z (A1), čtvrtá z (A4) a (A2), neboť prvek b je podle předpokladu také opačný k a. Poslední rovnost plyne opět z (A3) a komutativity (A2).

Vlastnosti 3. a 4. si můžete stejným způsobem dokázat sami. Všude nahradíte sčítání násobením a použijete odpovídající axiomy pro násobení.

5. Platí

$$0a = (0 + 0)a = 0a + 0a$$

podle axiomů (A3) a (D). Nyní k oběma stranám přičteme prvek $-(0a)$. Dostaneme

$$0 = -(0a) + 0a = -0a + (0a + 0a) = (-0a + 0a) + 0a = 0 + 0a = 0a.$$

První rovnost je důsledkem (A4), druhá je důsledkem předchozího výpočtu, třetí vyplývá z asociativity sčítání (A1), čtvrtá je důsledkem (A4) a poslední plyne z (A3).

6. Je-li $ab = 0$ a $a \neq 0$, můžeme tuto rovnost v důsledku axiomu (M4) vynásobit prvkem a^{-1}. Dostaneme pak

$$b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

První rovnost plyne z (M3), druhá z (M4), třetí z asociativity násobení (M1), čtvrtá je důsledkem předpokladu $ab = 0$ a pátou rovnost jsme dokázali v bodě 5.

7. Platí

$$0 = 0a = (-1 + 1)a = (-1)a + 1a = (-1)a + a.$$

První rovnost plýne z bodu 5. tohoto tvrzení, druhá je axiom (A4), třetí plyne z axiomu distributivity (D) a čtvrtá plyne z (M3). Dokázali jsme tak, že prvek $(-1)a$ je opačný k a. V důsledku jednoznačnosti prvku opačného k a dokázané v bodu 2. dostáváme rovnost $(-1)a = -a$.

8. Rovnost $ax = b$ můžeme kvůli předpokladu $a \neq 0$ vynásobit prvkem a^{-1}. Dostaneme

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b.$$

Jediným možným řešením rovnice je tedy prvek $x = a^{-1}b$. (Které axiomy a již dokázané vlastnosti jsme použili?) Dosazením $x = a^{-1}b$ do rovnice $ax = b$ zjistíme, že $a^{-1}b$ je skutečně řešením této rovnice.

Body 9., 10. a 12. si můžete dokázat sami.

11. Platí

$$(-a)(-b) = (-a)((-1)b) = ((-a)(-1))b = ((-1)(-a))b = (-(-a))b = ab.$$

Poslední rovnost vyplývá z faktu, že $-(-a) = a$ pro libovolný prvek $a \in \mathbf{T}$, což je důsledkem axiomu (A4) a jednoznačnosti opačného prvku dokázaného v 2. □

V každém tělese můžeme definovat operaci odečítání $a - b = a + (-b)$ a operaci dělení nenulovým prvkem b jako $a : b = ab^{-1}$.

Známými příklady těles jsou těleso racionálních čísel $\mathbf{Q}$, těleso reálných čísel $\mathbf{R}$ a těleso komplexních čísel $\mathbf{C}$. Ve všech případech počítáme s obvyklými operacemi sčítání a násobení čísel.

Příklad 4.3 *Dvouprvková množina* $\{0,1\}$ *spolu s operacemi sčítání*

$$0+0=1+1=0, \quad 0+1=1+0=1,$$

a násobení

$$1\cdot 1=1, \quad 0\cdot 1=1\cdot 0=0\cdot 0=0$$

je také těleso. Je to vlastně počítání modulo *2. Výsledek operace získáme tak, že uděláme napřed obvyklý součet dvou čísel a za výsledek pak vezmeme zbytek při dělení obvyklého součtu číslem 2. Podobně pro součin. Platnost všech axiomů tělesa můžeme pak ověřit přímo. Toto těleso budeme označovat* $\mathbf{Z}_2$.

Příklad 4.4 *Jiné konečné těleso dostaneme, když čísla* $\{0,1,2\}$ *sčítáme a násobíme* modulo *3. Operace sčítání je potom*

$$0+0=1+2=2+1=0,\ 0+1=1+0=2+2=1,\ 0+2=2+0=1+1=2,$$

a operace násobení je

$$0\cdot 0=0\cdot 1=1\cdot 0=0\cdot 2=2\cdot 0=0,\ 1\cdot 1=2\cdot 2=1,\ 1\cdot 2=2\cdot 1=2.$$

Můžete si sami ověřit, že množina $\{0,1,2\}$ *s takto definovanými operacemi je těleso. V případě asociativity obou operací a distributivity je třeba vždy ověřit* 27 *rovností.*

Příklad 4.5 *Množina* $\{0,1,2,3\}$ *spolu s operacemi sčítání a násobení* modulo *4* **není** *těleso. Platí v ní totiž* $2\cdot 2=0$ *a přitom* $2\neq 0$. *To se v žádném tělese nemůže stát podle Tvrzení 4.2.6.*

Příklad 4.6 *Čtyřprvkové těleso ale existuje. Nejlépe je počítat s polynomy* $\mathbf{GF}(4)=\{0,1,x,x+1\}$ *jedné proměnné s koeficienty* $0,1$. *Koeficienty považujeme za prvky tělesa* $\mathbf{Z}_2$. *Tyto polynomy pak můžeme sčítat a násobit obvyklým způsobem. Množina* $\mathbf{GF}(4)$ *je uzavřená na sčítání polynomů, není ale uzavřená na jejich násobení, neboť* $(x+1)(x+1)=x^2+(1+1)x+1=x^2+1$. *Operaci násobení proto definujeme* modulo *polynom* x^2+x+1. *To znamená, že obvyklý součin dvou polynomů vydělíme se zbytkem polynomem* x^2+x+1 *a jako výsledek součinu vezmeme tento zbytek. Potom platí např.*

$$x(x+1)=(x+1)x=1 \quad \text{a} \quad (x+1)(x+1)=x.$$

Zkuste si sami ověřit axiomy tělesa a dokázat, že množina $\mathbf{GF}(4)$ *je skutečně těleso.*

Příklad 4.7 *Množina* $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$ *pro* $n \geq 2$ *spolu s operacemi sčítání a násobení* modulo n *je těleso právě když je* n *prvočíslo. Toto tvrzení si nebudeme dokazovat. Pokud někdo zná Euklidův algoritmus, tak to zvládne sám. Jediný problém spočívá v důkazu existence inverzního prvku k libovolnému číslu* $0 \neq x < n$*, pokud je* n *prvočíslo. Pokud* n *není prvočíslo, tak* $\mathbf{Z}_n$ *není tělesem ze stejného důvodu, kvůli kterému není* $\mathbf{Z}_4$ *těleso.*

Příklad 4.8 *Pro každé prvočíslo* p *a každý exponent* $n \geq 1$ *existuje právě jedno těleso, které má* p^n *prvků a žádná jiná tělesa s konečným počtem prvků neexistují. Žádné šestiprvkové těleso tedy neeistuje. Tělesa s počtem prvků* p^n *pro* $n \geq 2$ *se konstruují podobně, jako jsme sestrojili čtyřprvkové těleso v Příkladu 4.6. Vezmeme všechny polynomy (včetně konstantních) stupně menšího než* n *s koeficienty v tělese* $\mathbf{Z}_p$*. Těch je celkem* p^n*. Na této množině sčítáme obvyklým způsobem a násobíme* modulo **vhodný** *polynom stupně* n*.*

V nějakém tělese $\mathbf{T}$ jsme definovali součet pouze *dvou* prvků. Chceme-li sečíst tři prvky $a, b, c \in \mathbf{T}$, musíme pomocí závorek určit, jaké dvojice prvků postupně sčítáme. Jsou dvě možnosti a axiom asociativity sčítání říká, že obě možnosti vedou ke stejnému výsledku. Podobně je tomu i u násobení. Následující tvrzení říká, že ani součet (součin) více než tří prvků nezávisí na uzávorkování.

Tvrzení 4.9 *V každém tělese* $\mathbf{T}$ *platí, že součet*

$$a_1 + a_2 + \cdots + a_n$$

nezávisí na uzávorkování, které k jeho výpočtu použijeme.

Podobně ani součin

$$a_1 a_2 \cdots a_n$$

nezávisí na uzávorkování, které k jeho výpočtu použijeme.

Důkaz. Budeme postupovat indukcí podle n. Důkaz uděláme pouze pro sčítání, pro násobení je zcela stejný. Pro $n = 1$ a $n = 2$ je tvrzení samozřejmé, pro $n = 3$ jde o axiom (A1).

Nechť je $n \geq 4$. Indukční předpoklad je, že součet méně než n prvků tělesa $\mathbf{T}$ nezávisí na uzávorkování. Uvažujme nyní dvě různá uzávorkování součtu $a_1 + a_2 + \cdots + a_n$. Při výpočtu podle prvního uzávorkování je poslední krok součet

$$(a_1 + \cdots + a_k) + (a_{k+1} + \cdots + a_n)$$

pro nějaké $0 < k < n$. V obou závorkách je součet méně než n prvků tělesa $\mathbf{T}$. Podle indukčního předpokladu je součet v každé z těchto dvou závorek nezávislý na uzávorkování. Nemusíme proto v žádné z obou závorek už vypisovat konkrétní uzávorkování.

Podobně je při výpočtu $a_1 + a_2 + \cdots + a_n$ podle druhého uzávorkování poslední krok

$$(a_1 + \cdots + a_l) + (a_{l+1} + \cdots + a_n)$$

pro nějaké $0 < l < n$.

Je-li $k = l$, vedou oba výpočty součtu $a_1 + a_2 + \cdots + a_n$ ke stejnému výsledku. Pokud je $k \neq l$, můžeme předpokládat, že např. $k < l$. Opět podle indukčního předpokladu můžeme napsat první výpočet jako

$$(a_1 + \cdots + a_k) + ((a_{k+1} + \cdots + a_l) + (a_{l+1} + \cdots + a_n)).$$

Podobně druhý výpočet můžeme napsat ve tvaru

$$((a_1 + \cdots + a_k) + (a_{k+1} + \cdots + a_l)) + (a_{l+1} + \cdots + a_n).$$

Oba výpočty tak vedou ke stejnému výsledku podle axiomu (A1). □

Vlastnosti těles hodně závisí na následujícím číselném parametru těles.

Definice 4.10 *Existuje-li kladné celé číslo n takové, že v tělese $\mathbf{T}$ platí*

$$\underbrace{1 + 1 + \cdots + 1}_{n} = 0,$$

pak nejmenší takové kladné číslo nazýváme charakteristika *tělesa $\mathbf{T}$.*

Pokud žádné takové kladné celé číslo n neexistuje, tak říkáme, že těleso $\mathbf{T}$ má charakteristiku 0.

Věta 4.11 *Charakteristika každého tělesa je buď 0 nebo prvočíslo.*

Důkaz. Jestliže charakteristika tělesa $\mathbf{T}$ není rovná 0, pak existuje nějaké kladné celé číslo $n \geq 2$, pro které platí

$$\underbrace{1 + 1 + \cdots + 1}_{n} = 0.$$

Jestliže je n složené číslo, platí $n = kl$ pro nějaká kladná celá čísla $k, l < n$. V důsledku axiomu distributivity (D) platí

$$(\underbrace{1 + 1 + \cdots + 1}_{k})(\underbrace{1 + 1 + \cdots + 1}_{l}) = \underbrace{1 + 1 + \cdots + 1}_{n} = 0.$$

Podle Tvrzení 4.2.6 může být součin dvou prvků v tělese rovný 0 pouze pokud je aspoň jeden z činitelů rovný 0. Proto je buď

$$\underbrace{1+1+\cdots+1}_{k}=0$$

nebo

$$\underbrace{1+1+\cdots+1}_{l}=0.$$

V každém případě nemůže být složené číslo $n \geq 2$ nejmenším kladným celým číslem, pro které platí

$$\underbrace{1+1+\cdots+1}_{n}=0.$$

Protože je $1 \neq 0$ podle axiomu netriviality (N), musí být nejmenší takové číslo prvočíslo. □

Cvičení 4.1 *Zjistěte charakteristiky těles* $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Q}$, $\mathbf{R}$ *a* $\mathbf{C}$. *Jakou má charakteristiku konečné těleso, které má* p^n *prvků?*

Konečná tělesa, zejména tělesa charakteristiky 2, hrají zcela základní roli v teorii *samoopravných kódů*, o kterých si řekneme více v některé z příštích kapitol. V této kapitole si ukážeme aplikaci v oblasti kryptologie. Ještě předtím jednu definici.

Definice 4.12 *Je-li* $\mathbf{T}$ *těleso a* $x_0, x_1, \ldots, x_{n-1} \in \mathbf{T}$, *pak matici*

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{pmatrix}$$

nazýváme Vandermondova *matice určená prvky* $x_0, x_1, \ldots, x_{n-1} \in \mathbf{T}$.

Základní vlastnost Vandermodových matic je obsahem následujícího tvrzení, které si dokážeme později.

Tvrzení 4.13 *Vandermondova matice určená prvky* $x_0, x_1, \ldots, x_{n-1} \in \mathbf{T}$ *je regulární právě když jsou prvky* $x_0, x_1, \ldots, x_{n-1}$ *navzájem různé.*

Secret sharing

Secret sharing, česky je asi nejvhodnější výraz *sdílení klíče*, je metoda, jak nějakou informaci rozdělit mezi $n \geq 2$ subjektů tak, aby ji mohlo rekonstruovat libovolných $k \leq n$ subjektů, ale žádných $k-1$ subjektů. Ukážeme si *Shamirovo schéma* pro sdílení klíče. Americký matematik Adi Shamir se proslavil především spoluautorstvím návrhu nejčastěji používaného systému šifrování s veřejným klíčem RSA. Písmeno S je v názvu právě kvůli Adi Shamirovi.

Shamirovo schéma pro sdílení klíče závisí na následujícím tvrzení, které je podstatným zobecněním Úlohy 1.1.

Tvrzení 4.14 *Buď $\mathbf{T}$ libovolné těleso obsahující aspoň $n \geq 2$ prvků. Nechť $x_0, x_1, \ldots, x_{n-1}$ je n navzájem různých prvků tělesa $\mathbf{T}$. Dále předpokládáme, že $b_0, b_1, \ldots, b_{n-1}$ jsou libovolné prvky tělesa $\mathbf{T}$. Potom existuje právě jedna funkce $f : \mathbf{T} \to \mathbf{T}$ definovaná předpisem*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} = \sum_{i=0}^{n-1} a_i x^i,$$

kde koeficienty $a_0, a_1, \ldots, a_{n-1} \in \mathbf{T}$ a hodnotu $f(x)$ počítáme v tělese $\mathbf{T}$, pro kterou platí

$$f(x_i) = b_i \quad \text{pro každé} \quad i = 0, 1, \ldots, n-1.$$

Důkaz. Pro každé $i = 0, 1, \ldots, n-1$ musí neznámé koeficienty $a_0, a_1, \ldots, a_{n-1}$ splňovat lineární rovnici

$$a_0 + a_1 x_i + a_2 x_i^2 + \cdots + a_{n-1} x_i^{n-1} = b_i.$$

Hledané koeficienty $a_0, a_1, \ldots, a_{n-1}$ tak musí vyhovovat soustavě n linárních rovnic o n neznámých

$$\begin{aligned} a_0 + a_1 x_0 + a_2 x_0^2 + \cdots + a_{n-1} x_0^{n-1} &= b_0 \\ a_0 + a_1 x_1 + a_2 x_1^2 + \cdots + a_{n-1} x_1^{n-1} &= b_1 \\ &\vdots \\ a_0 + a_1 x_{n-1} + a_2 x_{n-1}^2 + \cdots + a_{n-1} x_{n-1}^{n-1} &= b_{n-1}. \end{aligned}$$

Matice této soustavy je Vandermondova matice určená prvky $x_0, x_1, \ldots, x_{n-1}$. Podle Tvrzení 4.13 je matice soustavy regulární. Podle Věty 2.7 má tato soustava právě jedno řešení $a_0, a_1, \ldots, a_{n-1}$. □

Funkce $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ se nazývá polynom s koeficienty v tělese $\mathbf{T}$. Právě dokázané tvrzení tak říká, že existuje právě jeden polynom stupně $n-1$ s koeficienty v tělese $\mathbf{T}$, který má předepsané hodnoty v n různých bodech.

Jak využijeme Tvrzení 4.14 k rozdělení nějaké informace mezi n subjektů tak, aby ji mohlo rekonstruovat libovolných $k \leq n$ subjektů, ale žádných $k-1$ subjektů nemohlo získat žádnou relevantní informaci?

Zvolíme nějaké kódování možných informací pomocí prvků nějakého konečného tělesa $\mathbf{T}$, např. tělesa $\mathbf{Z}_p$, kde p je dostatečně velké prvočíslo. Pokud je informací, kterou chceme sdílet, třeba čtyřmístný PIN, stačí zvolit $p = 10007$, za předpokladu že $n < 10007$. Sdílené informaci odpovídá nějaký prvek $a_0 \in \mathbf{T}$. Zvolíme libovolný polynom s koeficienty v tělese $\mathbf{T}$ a stupně $k-1$:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}.$$

Všimněte si, že $f(0) = a_0$. Sdílenou informaci tak známe, pokud známe polynom $f(x)$. Nyní zcela náhodně vybereme n *nenulových* prvků $x_0, x_1, \ldots, x_{n-1} \in \mathbf{T}$. Subjektu i přidělíme informaci $x_i \in \mathbf{T}$ a $b_i = f(x_i) \in \mathbf{T}$ pro $i = 0, 1, \ldots, n-1$.

Pokud se sejde k subjektů, pak z jejich hodnot x_i a $b_i = f(x_i)$ můžeme rekonstruovat polynom f, neboť je to polynom stupně $k-1$, u kterého známe hodnoty v k různých bodech a takový polynom je podle Tvrzení 4.14 pouze jeden, tj. f. Absolutní člen tohoto polynomu je pak sdílená informace.

A co když se sejde pouze $k-1$ subjektů? Nemohou získat společně aspoň částečnou informaci o prvku $a_0 \in \mathbf{T}$? Pokud známe pouze $k-1$ hodnot x_i a b_i, můžeme si k nim přidat libovolný prvek $b \in \mathbf{T}$ a považovat jej za hodnotu hledaného polynomu v bodě 0. Podle Tvrzení 4.14 existuje právě jeden polynom g stupně $k-1$ s koeficienty v tělese $\mathbf{T}$, který má předepsané hodnoty b_i v $k-1$ bodech x_i a hodnotu b v bodě 0. Zde využíváme předokladu, že všechny prvky $x_0, x_1, \ldots, x_{n-1} \in \mathbf{T}$ jsou nenulové. Pro každou hodnotu sdílené informace b tak existuje právě jeden polynom g, který má absolutní člen rovný b a předepsané hodnoty v dalších $k-1$ bodech. Všechny možné hodnoty absolutního členu b jsou tedy stejně pravděpodobné a ze znalosti $k-1$ hodnot x_i a b_i tak nemůžeme získat žádnou relevantní informaci o prvku $a_0 \in \mathbf{T}$.