Ortogonalita a Hammingova vzdálenost v $\mathbb{F}^n$

Odpřednesenou látku naleznete v dodatku I skript *Abstraktní a konkrétní lineární algebra*.

Dnešní přednáška

1. Konečná tělesa tvaru $\mathbb{Z}_p$, kde p je prvočíslo.
2. Základy ortogonální geometrie v $\mathbb{F}^n$, kde $\mathbb{F}$ je obecné těleso.
3. Hammingova vzdálenost v $\mathbb{F}^n$.

Příští přednáška

1. Základy kódování v prostorech $(\mathbb{Z}_p)^n$ nad $\mathbb{Z}_p$, kde p je prvočíslo.

Připomenutí (viz druhou přednášku) — definice tělesa

Množině $\mathbb{F}$ spolu se dvěma operacemi sčítání $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, násobení $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, říkáme těleso, pokud jsou splněny následující podmínky:

1. Axiomy pro sčítání: sčítání je komutativní, asociativní a má neutrální prvek 0. Každý prvek má opačný prvek vzhledem ke sčítání.
2. Axiomy pro násobení: násobení je komutativní, asociativní a má neutrální prvek 1.
3. Distributivní zákony:[a] platí $a \cdot (b + c) = a \cdot b + a \cdot c$ a $(b + c) \cdot a = b \cdot a + c \cdot a$.
4. Test invertibility: $a \neq 0$ právě tehdy, když existuje a^{-1}.

[a] Díky komutativitě násobení stačí požadovat platnost pouze jednoho z distributivních zákonů.

Počítání modulo číslo

Zvolme přirozené číslo $m \geq 2$. Sčítání a násobení definujeme na zbytcích po dělení číslem m. Množinu zbytků označíme $\mathbb{Z}_m$. Například: pro $m = 4$ je $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Tabulky sčítání a násobení v $\mathbb{Z}_4$ jsou:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Například (jako zbytky): $2 + 3 = 5 = 1$, $2 \cdot 3 = 6 = 2$ v $\mathbb{Z}_4$.

Pozor: $3^{-1} = 3$ (protože $3 \cdot 3 = 1$), ale 2^{-1} neexistuje.

Tedy $\mathbb{Z}_4$ není těleso. Důvod: existuje $a \neq 0$, pro které neexistuje a^{-1}. Test invertibility je jediný z axiomů tělesa, který je v $\mathbb{Z}_4$ porušen.

Věta

$\mathbb{Z}_m$ je těleso právě tehdy, když m je prvočíslo.[a]

[a] Viz také Tvrzení 1.2.2 skript.

Důkaz.

1. Je-li $m = a \cdot b$ složené číslo ($a > 1$ a $b > 1$), potom $a \cdot b = 0$ v $\mathbb{Z}_m$, takže ani a ani b nemají inversi v $\mathbb{Z}_m$.
2. Je-li m prvočíslo, ukážeme indukcí, že každé číslo a z množiny $\{1, \ldots, m-1\}$ má v $\mathbb{Z}_m$ inversi.
   1. Je-li $a = 1$, pak $a^{-1} = 1$.
   2. Ať a splňuje $1 < a \leq m - 1$. Předpokládejme, že každé číslo z množiny $\{1, \ldots, a-1\}$ má v $\mathbb{Z}_m$ inversi.
      Vydělme m číslem a se zbytkem: $m = q \cdot a + a'$, kde $a' < a$ je zbytek po dělení. Protože m je prvočíslo, platí $a' \geq 1$. Potom platí $0 = q \cdot a + a'$ v $\mathbb{Z}_m$.
      Takže v Z_m platí $a' = (-q) \cdot a$. Protože a' má podle indukčního předpokladu inversi, platí v $\mathbb{Z}_m$ rovnost $1 = \underbrace{(a'^{-1} \cdot (-q))}_{=a^{-1}} \cdot a$.

Příklady těles tvaru $\mathbb{Z}_p$, p prvočíslo

1. Těleso $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

2. Těleso $\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Příklady těles tvaru $\mathbb{Z}_p$, p prvočíslo (pokrač.)

3. Násobení v tělese $\mathbb{Z}_{11}$ (vzpomeňte si na 10-ISBN):

$\cdot$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Poznámky k existenci prvočísel

1. Množina $\mathbb{P}$ všech prvočísel je nekonečná množina. Hledání velkých prvočísel je ale velmi obtížné.
2. The Great Internet Mersenne Prime Search.
   Ke dni 9. 2. 2024 je největším známým prvočíslem číslo

$$2^{82\,589\,933} - 1 \quad \text{(GIMPS, 7. 12. 2018)}$$

   Má 24 862 048 cifer.[a] Viz například stránky:
   1. http://primes.utm.edu/primes/
   2. http://www.mersenne.org/
3. O některých testech prvočíselnosti se lze dočíst například v textu J. Velebil, *Diskrétní matematika*, Praha, 2007.

[a] Jak vypadá binární zápis tohoto prvočísla? Uvědomme si, že každé číslo tvaru $2^k - 1$ má ve svém binárním zápise k jedniček.

Úplný popis konečných těles

Tělesa tvaru $\mathbb{Z}_p$, kde p je prvočíslo, netvoří úplný seznam konečných těles.
Vytvoření úplného seznamu konečných těles vyžaduje rozumět výpočtům v okruhu $\mathbb{Z}_p[x]$ (okruh polynomů nad $\mathbb{Z}_p$) modulo polynom.

Více například v textu

J. Velebil, *Diskrétní matematika*, Praha, 2007.

Obecná konečná tělesa umožňují studium dalších aplikací:

1. Cyklické kódy.
2. Šifrování na eliptických křivkách.
3. A řadu dalších.

Připomenutí skalárního součinu v $\mathbb{R}^n$ nad $\mathbb{R}$

Skalární součin $\langle - \mid - \rangle$ v $\mathbb{R}^n$ je funkce tvaru

$$\langle - \mid - \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$$

která splňuje tři podmínky:

1. Pro vš. $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{R}^n$ platí rovnost $\langle \mathbf{x} \mid \mathbf{y} \rangle = \langle \mathbf{y} \mid \mathbf{x} \rangle$.
2. Pro vš. $\mathbf{x}$ z $\mathbb{R}^n$ platí, že $\langle \mathbf{x} \mid - \rangle : \mathbb{R}^n \to \mathbb{R}$ je lineární zobrazení.
3. Pro vš. $\mathbf{x}$ z $\mathbb{R}^n$ platí $\langle \mathbf{x} \mid \mathbf{x} \rangle \geq 0$. Rovnost $\langle \mathbf{x} \mid \mathbf{x} \rangle = 0$ platí právě tehdy, když $\mathbf{x} = \mathbf{o}$.

Poznámka

Třetí podmínku šlo zformulovat, protože $\mathbb{R}$ je uspořádané těleso, tj. protože umíme rozpoznat nezáporná reálná čísla. Obecné těleso ale „rozumně“ uspořádat jít nemusí.[a]

[a] Např. těleso $\mathbb{C}$ uspořádat nelze, viz Příklad 1.3.8 skript. Viz také následující příklad.

Příklad (žádné konečné těleso $\mathbb{F}$ není uspořádané těleso)

Ať $\mathbb{F}$ je konečné těleso. V množině $\mathbb{F}$ nelze zadat podmnožinu $\mathbb{F}_+$ (množinu kladných prvků tělesa $\mathbb{F}$), která splňuje následující dvě podmínky:

1. Platí přesně jedna z podmínek $a = 0$, $a \in \mathbb{F}_+$, $-a \in \mathbb{F}_+$.
2. Jestliže $a \in \mathbb{F}_+$ a $b \in \mathbb{F}_+$, pak $a + b \in \mathbb{F}_+$ a $ab \in \mathbb{F}_+$.

Postupujeme sporem: ať taková množina $\mathbb{F}_+$ existuje.[a]
Protože $\mathbb{F}$ je konečná množina, existuje nejmenší kladné přirozené číslo n tak, že $\underbrace{1 + \cdots + 1}_{n\text{-krát}} = 0$.

Z axiomů pro $\mathbb{F}_+$ plyne, že platí $a^2 \in \mathbb{F}_+$ pro vš. $a \neq 0$.
Protože $1 = 1^2$, musí platit $1 \in \mathbb{F}_+$ a $\underbrace{1 + \cdots + 1}_{n\text{-krát}} \in \mathbb{F}_+$. To je spor.

[a] Množina $\mathbb{F}_+$ s těmito vlastnostmi umožňuje definovat uspořádání: $a < b$ iff $b - a \in \mathbb{F}_+$.

Tvrzení (vlastnosti zobrazení $\gamma : (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x}^T \cdot \mathbf{y}$ pro $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$)

Ať $\mathbb{F}$ je jakékoli těleso. Zobrazení $\gamma : (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x}^T \cdot \mathbf{y}$ z množiny $\mathbb{F}^n \times \mathbb{F}^n$ do množiny $\mathbb{F}$ se chová velmi podobně jako standardní skalární součin v $\mathbb{R}^n$. To jest, platí následující:

1. Pro vš. $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$ platí $\gamma(\mathbf{x}, \mathbf{y}) = \gamma(\mathbf{y}, \mathbf{x})$.
2. Pro vš. $\mathbf{x}$ z $\mathbb{F}^n$ je zobrazení $\gamma(\mathbf{x}, -) : \mathbb{F}^n \to \mathbb{F}$ lineární.

Podmínka

3. Rovnost $\gamma(\mathbf{x}, \mathbf{x}) = 0$ platí právě tehdy, když $\mathbf{x} = \mathbf{o}$.

ale obecně neplatí (protipříklad lze nalézt například v $(\mathbb{Z}_2)^2$).

Důkaz.

1. Protože $\gamma(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T \cdot \mathbf{y}$ a $\gamma(\mathbf{y}, \mathbf{x}) = \mathbf{y}^T \cdot \mathbf{x} = (\mathbf{x}^T \cdot \mathbf{y})^T$, platí[a] $\gamma(\mathbf{x}, \mathbf{y}) = \gamma(\mathbf{y}, \mathbf{x})$.

[a] Každá matice rozměrů 1×1 je totiž symetrická.

Důkaz (pokrač.).

2. Pro vš. $\mathbf{x}$ z $\mathbb{F}^n$ je zobrazení $\gamma(\mathbf{x}, -) : \mathbb{F}^n \to \mathbb{F}$ lineární, protože $\gamma(\mathbf{x}, a_1 \cdot \mathbf{y}_1 + a_2 \cdot \mathbf{y}_2) = \mathbf{x}^T \cdot (a_1 \cdot \mathbf{y}_1 + a_2 \cdot \mathbf{y}_2) = a_1 \cdot \mathbf{x}^T \cdot \mathbf{y}_1 + a_2 \cdot \mathbf{x}^T \cdot \mathbf{y}_2 = a_1 \cdot \gamma(\mathbf{x}, \mathbf{y}_1) + a_2 \cdot \gamma(\mathbf{x}, \mathbf{y}_2)$.
3. Pro $\mathbf{x} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ v $(\mathbb{Z}_2)^2$ platí $\gamma(\mathbf{x}, \mathbf{x}) = \mathbf{x}^T \cdot \mathbf{x} = 0$.

■

K čemu jsme použili positivní definitnost skalárních součinů?

Použili jsme ji pouze k důkazu C-S-B nerovnosti (tím pádem pro definici úhlu mezi vektory a pro definici normy a metriky vytvořené skalárním součinem).

Positivní definitnost jsme nepotřebovali pro definici ortogonality.

Připomenutí: vektory $\mathbf{x}$, $\mathbf{y}$ v $\mathbb{R}^n$ jsou ortogonální (vzhledem ke skalárnímu součinu $\langle - \mid - \rangle$), pokud platí $\langle \mathbf{x} \mid \mathbf{y} \rangle = 0$.

Definice (ortogonalita v $\mathbb{F}^n$)

Řekneme, že vektory $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$ jsou ortogonální[a] (také: navzájem na sebe kolmé), pokud platí $\mathbf{x}^T \cdot \mathbf{y} = 0$.

[a] Přesněji: v $\mathbb{F}^n$ jde o ortogonalitu vzhledem k $\gamma(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T \cdot \mathbf{y}$.
Slogan: ortogonalita v $\mathbb{F}^n$ zobecňuje ortogonalitu vzhledem ke standardnímu skalárnímu součinu v $\mathbb{R}^n$.

Definice (ortogonální doplněk lineárního podprostoru $\mathbb{F}^n$)

Pro lineární podprostor W prostoru $\mathbb{F}^n$ definujeme jeho ortogonální doplněk jako množinu

$$W^\perp = \{\mathbf{x} \in \mathbb{F}^n \mid \mathbf{w}^T \cdot \mathbf{x} = 0 \text{ pro všechna } \mathbf{w} \text{ z } W\}$$

Poznámka

Protože $\mathbf{w}^T \cdot \mathbf{x} = 0$ iff $\mathbf{x}^T \cdot \mathbf{w} = 0$, platí

$$W^\perp = \{\mathbf{x} \in \mathbb{F}^n \mid \mathbf{x}^T \cdot \mathbf{w} = 0 \text{ pro všechna } \mathbf{w} \text{ z } W\}$$

Věta (vlastnosti ortogonálního doplňku)

Ať W je lineární podprostor prostoru $\mathbb{F}^n$. Potom platí:

1. $W^\perp$ je opět lineární podprostor prostoru $\mathbb{F}^n$.
2. Je-li $\dim(W) = k$, pak $\dim(W^\perp) = n - k$.
3. Platí $(W^\perp)^\perp = W$.

Důkaz.

1.
   1. Pro všechna $\mathbf{w}$ z W platí $\mathbf{w}^T \cdot \mathbf{o} = 0$. Tudíž $\mathbf{o}$ je ve $W^\perp$.
   2. Jestliže $\mathbf{x}_1$ a $\mathbf{x}_2$ jsou ve $W^\perp$, pak
   $$\mathbf{w}^T \cdot (a_1 \cdot \mathbf{x}_1 + a_2 \cdot \mathbf{x}_2) = a_1 \cdot \underbrace{\mathbf{w}^T \cdot \mathbf{x}_1}_{=0} + a_2 \cdot \underbrace{\mathbf{w}^T \cdot \mathbf{x}_2}_{=0} = 0$$
   pro všechna $\mathbf{w}$ ve W. Ukázali jsme, že $W^\perp$ je uzavřen v $\mathbb{F}^n$ na tvorbu lineárních kombinací.

   Takže $W^\perp$ je lineární podprostor[a] prostoru $\mathbb{F}^n$.

[a] Elegantní důkaz téhož: $W^\perp = \bigcap_{\mathbf{w} \in W} \ker(\gamma(\mathbf{w}, -))$, kde $\gamma(\mathbf{w}, \mathbf{x}) = \mathbf{w}^T \cdot \mathbf{x}$.

Důkaz (pokrač.).

2. Označme jako $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ uspořádanou bázi W. Pro matici $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_k)$ platí: $\mathbf{x}$ je ve $W^\perp$ iff $\mathbf{A}^T \cdot \mathbf{x} = \mathbf{o}$ iff $\mathbf{x}$ je v $\ker(\mathbf{A}^T)$. Neboli: $W^\perp = \ker(\mathbf{A}^T)$.

   Protože $\mathrm{rank}(\mathbf{A}^T) = \mathrm{rank}(\mathbf{A}) = k$ a protože $\mathbf{A}^T : \mathbb{F}^n \to \mathbb{F}^k$, je $\mathrm{def}(\mathbf{A}^T) = n - k$ podle věty o dimensi jádra a obrazu.

   To znamená, že $\dim(W^\perp) = n - k$.

3. Zjevně platí $W \subseteq (W^\perp)^\perp$, protože každý vektor $\mathbf{w}$ z W je ortogonální ke každému vektoru z $W^\perp$.

   Je-li $\dim(W) = k$, je $\dim((W^\perp)^\perp) = n - (n - k) = k$.

   Proto $W = (W^\perp)^\perp$.

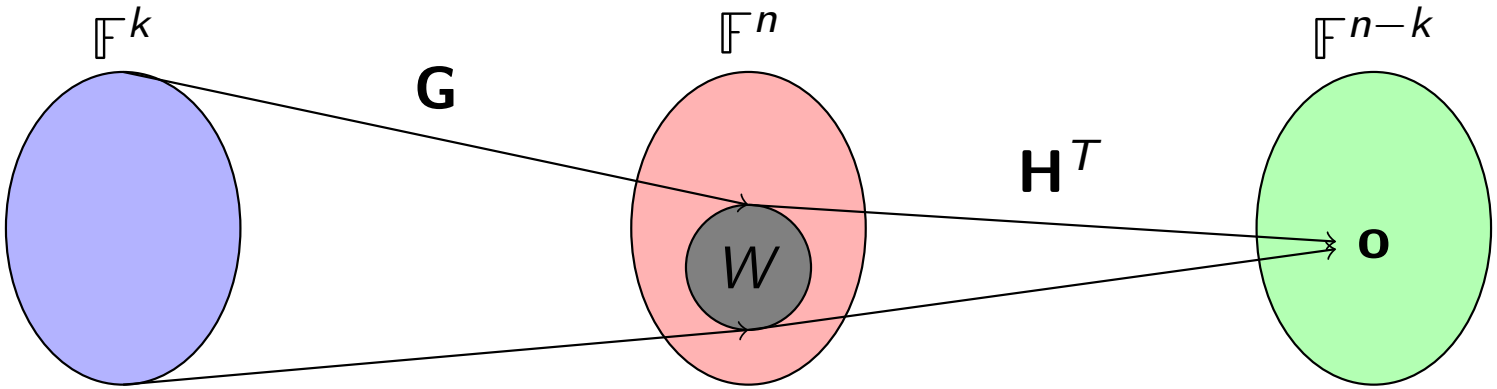
Příklad (rovnost $W = W^\perp$ může platit)

Pro podmnožinu $W = \{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\}$ lineárního prostoru $(\mathbb{Z}_2)^2$ platí:[a]

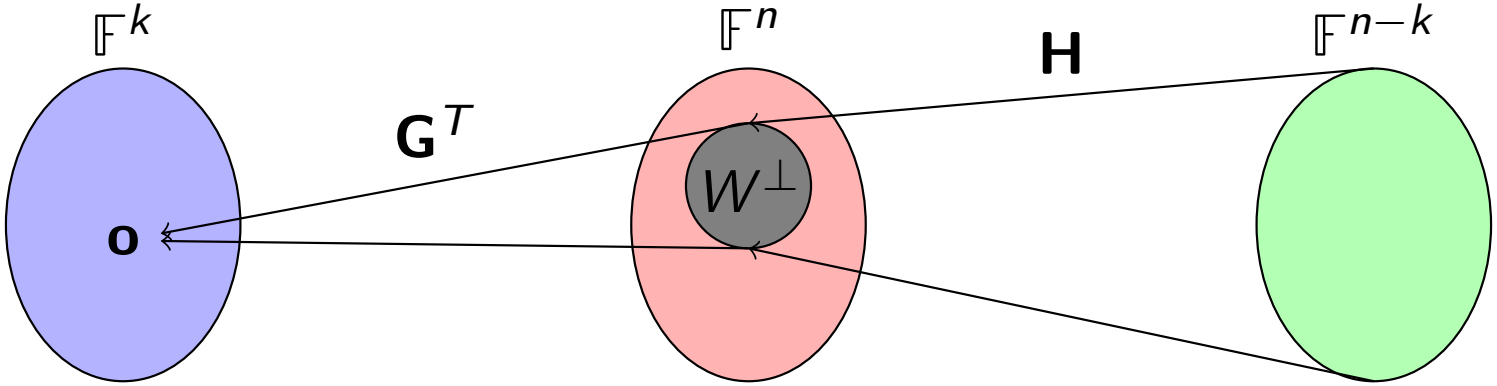
1. W je lineární podprostor prostoru $(\mathbb{Z}_2)^2$.
2. $W = \text{span}(\begin{pmatrix}1\\1\end{pmatrix})$, $\dim(W) = 1$.
3. $$\begin{aligned} W^\perp &= \{\begin{pmatrix}x_1\\x_2\end{pmatrix} \mid \begin{pmatrix}0\\0\end{pmatrix}^T \cdot \begin{pmatrix}x_1\\x_2\end{pmatrix} = 0 \text{ a současně } \begin{pmatrix}1\\1\end{pmatrix}^T \cdot \begin{pmatrix}x_1\\x_2\end{pmatrix} = 0\} \\ &= W \end{aligned}$$

[a] Pro zájemce (nepovinné): „absurdní“ rovnost $W = W^\perp$ je způsobena degenerovaností podprostoru W prostoru $(\mathbb{Z}_2)^2$. Všechny vektory podprostoru W jsou totiž na sebe navzájem kolmé.

Dualita generujících a kontrolních matic podprostoru



$$\mathrm{im}(\mathbf{G}) = W = \ker(\mathbf{H}^T)$$



$$\mathrm{im}(\mathbf{H}) = W^\perp = \ker(\mathbf{G}^T)$$

Definice (Hammingova vzdálenost v $\mathbb{F}^n$)

Pro vektory $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$ definujeme

$$d_H(\mathbf{x}, \mathbf{y}) = \text{ počet různých položek vektorů } \mathbf{x} \text{ a } \mathbf{y}$$

Přirozenému číslu $d_H(\mathbf{x}, \mathbf{y})$ říkáme Hammingova vzdálenost vektorů $\mathbf{x}$ a $\mathbf{y}$.

Poznámka

Pro všechny vektory $\mathbf{x}$, $\mathbf{y}$ z $\mathbb{F}^n$ platí $d_H(\mathbf{x}, \mathbf{y}) \leq n$.

Tvrzení (Hammingova vzdálenost je metrika na $\mathbb{F}^n$)

Pro všechny vektory $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ z $\mathbb{F}^n$ platí:

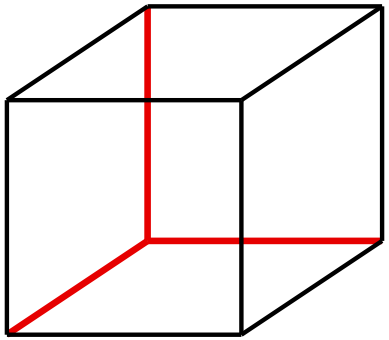
1. $d_H(\mathbf{x}, \mathbf{y}) \geq 0$, rovnost nastává právě tehdy, když $\mathbf{x} = \mathbf{y}$.
2. $d_H(\mathbf{x}, \mathbf{y}) = d_H(\mathbf{y}, \mathbf{x})$.
3. $d_H(\mathbf{x}, \mathbf{y}) \leq d_H(\mathbf{x}, \mathbf{z}) + d_H(\mathbf{z}, \mathbf{y})$.

Důkaz.

Důkaz plyne okamžitě z definice d_H. ∎

Příklad (Hammingova vzdálenost v $(\mathbb{Z}_2)^3$)

Osm vektorů $\begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}$ prostoru $(\mathbb{Z}_2)^3$ si lze představit jako vrcholy krychle (červené hrany jsou souřadnicové osy):



Hammingova vzdálenost dvou vektorů je pak délka nejkratší cesty po hranách krychle z jednoho vrcholu do druhého.

Podobnou představu lze mít o Hammingově vzdálenosti vektorů v prostoru $(\mathbb{Z}_2)^n$: vektory v $(\mathbb{Z}_2)^n$ jsou vrcholy n-dimensionální krychle.