Lineární kódy

2. přednáška z algebraického kódování

Obsah

Bezpečnostní kódy

- Bezpečnostní kódy odhalují, zda při přenosu nedošlo k chybě, případně chyby opravují.
- K informačním znakům musíme přidat kontrolní znaky. Čím více chyb chceme odhalit, tím více kontrolních znaků musíme přidat.
- Chceme sestrojit kódy, které budou odhalovat daný počet chyb a přitom budou mít rozumně nízkou redundanci. Navíc chceme, aby tyto kódy měly jednoduchý algoritmus opravování chyb.

Bezpečnostní kódy

- Pokud na konečné kódové abecedě T budeme umět sčítat a násobit tak, aby T bylo těleso, pak množina T^n všech slov délky n bude lineární prostor a budeme moci použít aparát lineární algebry.
- Lineární prostory nad obecným tělesem se "chovají podobně" jako lineární prostory nad tělesem reálných čísel.

Lineární prostor nad tělesem

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 $\bar{u}, \bar{v} \in L$:
  - $\alpha \boxdot (\bar{u} \oplus \bar{v}) = (\alpha \boxdot \bar{u}) \oplus (\alpha \boxdot \bar{v})$
  - $(\alpha + \beta) \boxdot \bar{u} = (\alpha \boxdot \bar{u}) \oplus (\beta \boxdot \bar{u})$
  - $(\alpha \cdot \beta) \boxdot \bar{u} = \alpha \boxdot (\beta \boxdot \bar{u})$
  - $1 \boxdot \bar{u} = \bar{u}$

Operace sčítání a číselného násobku budeme dále značit jen $+$ a $\cdot$.

Lineární prostor všech slov délky n nad T

Nechť T je konečné těleso. Množina všech slov délky n nad T

$$T^n = \{\bar{u} = (u_1 u_2 \dots u_n),\ u_i \in T\}$$

tvoří lineární prostor nad tělesem T.

Sčítání a násobení číslem $a \in T$ je definováno po složkách,

$$\bar{u} + \bar{v} = (u_1 + v_1 \dots u_n + v_n), \quad a \cdot \bar{u} = (au_1 \dots au_n),$$

kde "písmena" se sčítají a násobí v T. Počet slov je $|T|^n$.

Poznámka

Pro přehlednost budeme slova dávat do závorek, neboť to je obvyklé značení vektorů v lineární algebře.

Lineární podprostory

- *Podprostor* lineárního prostoru L je neprázdná podmnožina $P \subseteq L$, která je uzavřená na sčítání a číselné násobky.
- Podprostor musí vždy obsahovat nulový vektor daného prostoru.
- *Báze* lineárního podprostoru P je jeho lineárně nezávislá podmnožina $B = \{\bar{b}_1, \ldots, \bar{b}_k\}$, která generuje celý prostor P. Báze budeme chápat jako uspořádané báze.
- Počet prvků (libovolné) báze podprostoru P se nazývá *dimenze* podprostoru P, zde $\dim P = k$.

Lineární podprostory

- Každý vektor z P lze právě jedním způsobem nakombinovat z bázických vektorů:

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

- Jednoznačně určená k-tice koeficientů $(a_1 \dots a_k) \in T^k$ se nazývá *souřadnice* vektoru $\bar{u}$ vzhledem k bázi B.
- Přechod od vektorů z podprostoru P k jejich souřadnicím v T^k je lineární zobrazení, které je vzájemně jednoznačné, tzv. *isomorfismus*.

Skoro skalární součin na T^n

Nechť T je konečné těleso.

- Zobrazení $\odot : T^n \times T^n \to T$ definované předpisem:

$$\bar{u} \odot \bar{v} = u_1 v_1 + \ldots u_n v_n$$

  je symetrická bilineární forma. Budeme mluvit o *skoro skalárním součinu* na T^n.
- *Kolmost* slov: $\bar{u} \perp \bar{v}$, když $\bar{u} \odot \bar{v} = 0$.
- *Kolmý doplněk* k podprostoru P v prostoru T^n je množina $P^\perp = \{\bar{u} \in T^n;\ \bar{u} \perp \bar{v} \text{ pro všechna } \bar{v} \in P\}$.
  Kolmý doplněk $P^\perp$ tvoří podprostor, $\dim P^\perp = n - \dim P$.

Skoro skalární součin na T^n

Poznámka

- Skalární součin v lineárním prostoru L je bilineární forma, která je symetrická a pozitivně definitní.
- Naše zobrazení nesplňuje pozitivní definitnost:
  pro všechna $\bar{u} \in L$ je $\bar{u} \odot \bar{u} \geq 0$ a rovnost nastane právě, když $\bar{u} = \bar{o}$.
- Příčina: 1) Konečná tělesa neumíme uspořádat.
  Je v $\mathbb{Z}_3$ číslo $2 = -1$ větší či menší než číslo 0?
  2) Např. pro $\bar{u} = (1 \ldots 1) \neq \bar{o} \in \mathbb{Z}_p^p$ je $\bar{u} \odot \bar{u} = 0$ v $\mathbb{Z}_p$.
- Důsledek: Selhává geometrická představa kolmosti, vektor může být kolmý sám na sebe.

Soustavy lineárních rovnic nad $\mathbb{Z}_p$

- *Soustavy lineárních rovnic* nad $\mathbb{Z}_p$ se řeší stejně jako nad $\mathbb{R}$ a jako nad jakýmkoliv tělesem T.
- Nad $\mathbb{Z}_p$ funguje *Gaussova eliminační metoda*. Místo dělení rovnice vedoucím pivotem používá násobení k němu inverzním prvkem. (V $\mathbb{Z}_p$ má každé nenulové číslo inverzní prvek.)
- Poznámka: Nad $\mathbb{Z}_n$, kde n není prvočíslo, obecně Gaussova eliminace nefunguje.

Soustavy lineárních rovnic nad $\mathbb{Z}_p$

- Soustavu m lineárních rovnic o n neznámých můžeme zapsat maticově: $\mathbb{A}\bar{x}^T = \bar{b}^T$, kde $\mathbb{A}$ je matice nad $\mathbb{Z}_p$ typu (m, n).
- Řešením je každá $n-$tice $\bar{a} \in \mathbb{Z}_p^n$, která vyhovuje všem rovnicím. Soustava může mít jedno řešení, žádné řešení, nebo p^k různých řešení, kde $k = m - \operatorname{hod} \mathbb{A}$ je počet proměnných, které smíme volit libovolně v $\mathbb{Z}_p$.

Tvrzení - struktura množiny všech řešení

1. Všechna řešení homogenní soustavy $\mathbb{A}\bar{x}^T = \bar{o}^T$ nad $\mathbb{Z}_p$ o n neznámých tvoří podprostor v $\mathbb{Z}_p^n$.
2. Každé řešení (ne)homogenní soustavy rovnic $\mathbb{A}\bar{x}^T = \bar{b}^T$ je součtem partikulárního řešení této soustavy a nějakého řešení přidružené homogenní soustavy.

Podprostory a soustavy lineárních rovnic

Tvrzení - popis podprostoru

Každý podprostor P v lineárním prostoru $\mathbb{Z}_p^n$ můžeme popsat homogenní soustavou lineárních rovnic, aneb pro vhodnou matici $\mathbb{A}$ platí:

$$\bar{u} \in P \quad \text{iff} \quad \bar{u} \text{ řeší soustavu } \mathbb{A}\bar{x}^T = \bar{o}^T$$

Jak najít matici této soustavy? Následující tvrzení jsou ekvivalentní:

- $\bar{u}$ řeší homogenní soustavu $\mathbb{A}\bar{x}^T = \bar{o}^T$
- $R_i \odot \bar{u} = 0$ pro každý řádek R_i matice $\mathbb{A}$
- $R_i \perp \bar{u}$ pro každý řádek R_i matice $\mathbb{A}$

Podprostory a soustavy lineárních rovnic

Tvrzení

Nechť podprostor P v prostoru $\mathbb{Z}_p^n$ má bázi $B = \{\bar{b}_1, \ldots, \bar{b}_k\}$ a nechť $C = \{\bar{c}_1, \ldots, \bar{c}_{n-k}\}$ je báze ortogonálního doplňku $P^\perp$. Protože $(P^\perp)^\perp = P$, tak platí:

- Podprostor P je množinou všech řešení soustavy $\mathbb{A}\bar{x}^T = \bar{o}^T$, kde matice $\mathbb{A}$ má v řádcích bázické vektory $\bar{c}_1, \ldots, \bar{c}_{n-k}$ podprostoru $P^\perp$.
- Podprostor $P^\perp$ je množinou všech řešení soustavy $\mathbb{B}\bar{x}^T = \bar{o}^T$, kde matice $\mathbb{B}$ má v řádcích bázické vektory $\bar{b}_1, \ldots, \bar{b}_k$ podprostoru P.
- Aneb bázi jednoho z podprostorů P, $P^\perp$ určíme jako bázická řešení homogenní soustavy s maticí, která má v řádcích bázi druhého podprostoru.

Maticový počet nad $\mathbb{Z}_n$

Maticový počet lze dělat nad okruhem $\mathbb{Z}_n$, i když některé záležitosti budou fungovat jinak než nad $\mathbb{R}$.

- Čtvercová matice $\mathbb{A}$ je *regulární matice* nad $\mathbb{Z}_n$, když $\det \mathbb{A}$ je invertibilní v $\mathbb{Z}_n$.
- Pouze regulární matice $\mathbb{A}$ má *inverzní matici* nad $\mathbb{Z}_n$.

$$\mathbb{A}^{-1} = (\det \mathbb{A})^{-1} \mathbb{D}^T$$

$\mathbb{D} = ((-1)^{i+j} \det \mathbb{A}_{ij})$, kde $\mathbb{A}_{ij}$ vznikla vyškrtnutím i-tého řádku a j-tého sloupce, je matice algebraických doplňků k $\mathbb{A}$.

- Nad $\mathbb{Z}_p$ funguje Gaussova eliminace, je tudíž možné počítat inverzní matici eliminací na řádky dvojmatice: $(\mathbb{A}|\mathbb{E}) \sim \ldots \sim (\mathbb{E}|\mathbb{A}^{-1})$, kde $\mathbb{E}$ je jednotková matice.

Maticový počet nad $\mathbb{Z}_n$

- Pro matici $\mathbb{A}$ typu (m, n) nad $\mathbb{Z}_n$ definujeme *řádkovou hodnost* jako dimenzi podprostoru generovaného řádky matice $\mathbb{A}$ a *sloupcovou hodnost* jako dimenzi podprostoru generovaného sloupci matice $\mathbb{A}$.
- Protože nad $\mathbb{Z}_n$ obecně nefunguje Gaussova eliminační metoda, řádková hodnost matice $\mathbb{A}$ se nemusí rovnat sloupcové hodnosti matice $\mathbb{A}$.
- Nad $\mathbb{Z}_p$ se dá dokázat díky Gaussově eliminaci, že se tyto hodnosti rovnají, a je možné definovat pojem *hodnost matice* $\mathbb{A}$.

Lineární kódy

Kód je množina všech *kódových slov*.
Blokový kód délky n nad $\mathbb{Z}_p$ je kód, jehož slova mají délku n, abeceda je p-znaková množina $\mathbb{Z}_p$.

Definice

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

Příklady lineárních kódů

- Opakovací kód délky 3 nad $\mathbb{Z}_2$, $K = \{(000), (111)\}$.
- Kód kontroly parity délky 3 nad $\mathbb{Z}_2$, $K = \{(000), (011), (101), (110)\}$.

Lineární kódy

Pozorování

Nechť K je lineární (n, k)-kód nad $\mathbb{Z}_p$.

- Nulové slovo je vždy kódové, $\bar{o} \in K$.
- K obsahuje p^k kódových slov.
- k je počet informačních znaků a $m = n - k$ je počet kontrolních znaků kódu K (viz dále).

Kódování

Nechť K je (lineární) kód nad $\mathbb{Z}_p$.
Kódování je prosté zobrazení $\varphi : \mathbb{Z}_p^k \to K$, které každému informačnímu slovu délky k přiřadí kódové slovo.
Každý kód může mít více možností kódování.

Příklad

Opakovací kód délky 3 nad $\mathbb{Z}_2$, $K = \{(000), (111)\}$,
má (systematické lineární) kódování: $0 \mapsto (000)$, $1 \mapsto (111)$.
Také $1 \mapsto (000)$, $0 \mapsto (111)$ je kódování, ale není lineární.
Dva znaky jsou kontrolní a umožňují objevit dvě chyby a opravit jednu chybu.

Kódování

Nechť $B = \{\bar{b}_1, \ldots, \bar{b}_k\}$ je báze lineárního (n, k)-kódu K.

$$\varphi : \mathbb{Z}_p^k \to K : \bar{a} = (a_1 \ldots a_k) \mapsto \bar{v} = \sum_{i=1}^{k} a_i \bar{b}_i$$

je vzájemně jednoznačné lineární zobrazení (isomorfismus).

Zobrazení φ určuje kódování informačních slov délky $k = \dim K$.
Informační znaky jsou souřadnice kódového slova vůči bázi B.

Naopak, každé lineární kódování $\psi : \mathbb{Z}_p^k \to K$ jednoznačně určuje bázi kódu K, tvoří ji obrazy standardní báze v prostoru $\mathbb{Z}_p^k$.

Kódování

Generující matice

Nechť $B = \{\bar{b}_1, \ldots, \bar{b}_k\}$ je báze lineárního (n, k)-kódu K.

Matice $\mathbb{G} = \begin{pmatrix} \bar{b}_1 \\ \vdots \\ \bar{b}_k \end{pmatrix}$ se nazývá *generující matice* kódu K.

Kódování se provádí vynásobením informačního slova generující maticí:

$$\varphi : \mathbb{Z}_p^k \to K : \bar{a} \mapsto \bar{a} \cdot \mathbb{G} = \bar{v}$$

Poznámka

Gaussova eliminace na řádky převede generující matici $\mathbb{G}$ kódu K na jinou generující matici $\mathbb{G}'$ téhož kódu K.

Kódování

Dekódování informačních znaků

Dekódování coby inverzní zobrazení $\varphi^{-1} : K \to \mathbb{Z}_p^k$ probíhá takto:

- pro slovo $\bar{v} \in K$ hledáme jeho souřadnice vůči bázi, která je v řádcích matice $\mathbb{G}$.
- Musíme vyřešit soustavu $\mathbb{G}^T \bar{a}^T = \bar{v}^T$
  n lineárních rovnic o k neznámých, kde $\operatorname{hod} \mathbb{G}^T = k$
  a soustava má řešení (neboť $\bar{v} \in K$).
- Můžeme se omezit na k lineárně nezávislých rovnic a vyřešit danou podsoustavu s regulární maticí (např. tak, že ji vynásobíme inverzní maticí).

Systematické kódování

Nechť K je lineární $(n, k)-$ kód nad $\mathbb{Z}_p$.
Systematické kódování je kódování, které ponechá informační znaky na začátku kódového slova a doplní je o kontrolní znaky:

$$\varphi : \mathbb{Z}_p^k \to K : \bar{a} = (a_1 \dots a_k) \mapsto \bar{v} = (a_1 \dots a_k\, b_1 \dots b_{n-k})$$

Systematická generující matice kódu K je jeho generující matice tvaru $\mathbb{G}_S = \left(\mathbb{E}_k\, \mathbb{B}\right)$.

Systematické kódování má snadné dekódování informačních znaků:

$$\varphi^{-1} : K \to \mathbb{Z}_p^k : \bar{v} = (v_1 \dots v_n) \mapsto \bar{a} = (v_1 \dots v_k)$$

Pokud to půjde, budeme chtít kódovat systematicky.

Systematické kódování

Kód, který má systematické kódování, se nazývá systematický kód.

Tvrzení

Ke každému lineárnímu kódu K lze najít systematický lineární kód K', který se liší pouze v pořadí znaků.

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.
Permutací znaků lze udělat systematický kód
$K' = \{(a\,b\,c\,a\,b\,c), a, b, c \in \mathbb{Z}_2\}$.

Kódování

Příklady

- Opakovací kód délky 3 nad $\mathbb{Z}_2$, $K = \{(000), (111)\}$, má systematickou generující matici $\mathbb{G}_S = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.
- Kód kontroly parity délky 3 nad $\mathbb{Z}_2$, $K = \{(000), (011), (101), (110)\}$, má systematickou generující matici $\mathbb{G}_S = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.
- Kód kontroly parity délky 3 nad $\mathbb{Z}_2$, má také generující matici $\mathbb{G} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$. Ta určuje nesystematické kódování: $(00) \mapsto (000)$, $(01) \mapsto (101)$, $(10) \mapsto (110)$, $(11) \mapsto (011)$.

Objevování chyb

Kontrolní matice

Nechť K je lineární $(n, k)-$ kód nad $\mathbb{Z}_p$.
Lineární podprostor K lze popsat soustavou lineárních rovnic.
Buď $C = \{\bar{c}_1, \ldots, \bar{c}_{n-k}\}$ báze podprostoru $K^\perp$, pak

$$\bar{v} \in K \quad \text{iff} \quad \mathbb{H}\,\bar{v}^T = \bar{o}^T \ \text{ pro } \ \mathbb{H} = \begin{pmatrix} \bar{c}_1 \\ \vdots \\ \bar{c}_{n-k} \end{pmatrix}.$$

Matice $\mathbb{H}$ se nazývá *kontrolní matice* kódu K.

Poznámka

Gaussova eliminace na řádky převede kontrolní matici $\mathbb{H}$ kódu K na jinou kontrolní matici $\mathbb{H}'$ téhož kódu K.

Objevování chyb

Kontrola přijatého slova

Bylo vysláno slovo $\bar{v} \in K \subseteq \mathbb{Z}_p^n$ a přijato slovo $\bar{w} \in \mathbb{Z}_p^n$.
Pokud $\mathbb{H}\,\bar{w}^T \neq \bar{o}^T$, pak $\bar{w} \notin K$, tudíž $\bar{v} \neq \bar{w}$.
Při přenosu jistě došlo k chybě.
V opačném případě je $\bar{w} \in K$ a předpokládáme, že $\bar{v} = \bar{w}$.

Pomocí kontrolní matice lze někdy chybu i opravit, jak uvidíme později.

Objevování chyb

Vztah mezi generující a kontrolní maticí

Nechť lineární kód K má generující matici $\mathbb{G}$ a kontrolní matici $\mathbb{H}$. Pak platí:

- $\mathbb{G}$ má v řádcích bázická řešení soustavy $\mathbb{H}\,\bar{x}^T = \bar{o}^T$
- $\mathbb{H}$ má v řádcích bázická řešení soustavy $\mathbb{G}\,\bar{x}^T = \bar{o}^T$

Tvrzení

Má-li lineární $(n, k)-$kód K generující matici $\mathbb{G}_S = \left(\mathbb{E}_k\, \mathbb{B}\right)$, pak má kontrolní matici $\mathbb{H} = \left(-\mathbb{B}^T\, \mathbb{E}_{n-k}\right)$.

Objevování chyb

Příklady

- Opakovací kód délky 3 nad $\mathbb{Z}_2$ je popsán rovnicemi $v_1 = v_2$, $v_1 = v_3$, což odpovídá kontrolní matici
$$\mathbb{H} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$
- Kód kontroly parity délky 3 nad $\mathbb{Z}_2$ je popsán rovnicí $v_1 + v_2 + v_3 = 0$, má tedy kontrolní matici $\mathbb{H} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

Duální kódy

Duální kód

Nechť K je lineární $(n, k)-$kód nad $\mathbb{Z}_p$ s generující maticí $\mathbb{G}$ a kontrolní maticí $\mathbb{H}$.
Lineární $(n, n-k)-$kód $K^{\perp}$ nad $\mathbb{Z}_p$ se nazývá *duální kód* kódu K.

Kód $K^{\perp}$ má generující matici $\mathbb{H}$ a kontrolní matici $\mathbb{G}$.

Příklady

Opakovací kód délky n nad $\mathbb{Z}_p$ a kód kontroly parity délky n nad $\mathbb{Z}_p$ (určený rovnicí: součet písmen je nula v $\mathbb{Z}_p$) jsou navzájem duální kódy.

Dekódování

Dekódování přijatého slova

Nechť K je lineární $(n, k)-$kód nad $\mathbb{Z}_p$.
Bylo vysláno slovo $\bar{v} \in K$ a přijato slovo $\bar{w} \in \mathbb{Z}_p^n$.

- Dekódování je zobrazení $\delta : \mathbb{Z}_p^n \to K$. Jedná se vlastě o opravení přijatého slova na slovo kódové.
- Částečné dekódování je zobrazení $\delta : M \to K$, kde $K \subseteq M \subseteq \mathbb{Z}_p^n$. Například chceme opravit jen ta přijatá slova, která mají jednoznačnou opravu.

Pozor: Rozlišujeme "dekódování přijatého slova" a "dekódování informačních znaků" z kódového slova.
Pokud budeme mluvit o dekódování, budeme tím myslet dekódování přijatého slova na slovo kódové.

Dekódování

- Předpokládáme, že pravděpodobnost, že při přenosu dojde k chybě, je malá. Např. u binárního symetrického kanálu je pravděpodobnost chyby menší než $\frac{1}{2}$.
- Potom je pravděpodobnost, že došlo méně chybám, větší než pravděpodobnost, že došlo k více chybám.
- Při dekódování budeme hledat kódové slovo, které se od přijatého slova liší v co nejméně znacích (= nejbližšího souseda). Toto je tzv. "nearest neighbour decoding".

Hammingova vzdálenost

Definice

Hammingova váha slova $\bar{u}$ je rovna počtu nenulových znaků ve slově $\bar{u}$. Značíme $\|\bar{u}\|_H$.
Hammingova vzdálenost slov $\bar{u}$ a $\bar{v}$ délky n je rovna počtu znaků, ve kterých se obě slova liší, aneb $d_H(\bar{u}, \bar{v}) = \|\bar{v} - \bar{u}\|_H$.

Tvrzení

Hammingova vzdálenost je metrikou na množině $\mathbb{Z}_p^n$.
Pro všechna $\bar{u}, \bar{v}, \bar{w} \in \mathbb{Z}_p^n$ platí:

- $d_H(\bar{u}, \bar{v}) \geq 0$ a rovnost nastane právě, když $\bar{u} = \bar{v}$
- $d_H(\bar{u}, \bar{v}) = d_H(\bar{v}, \bar{u})$
- $d_H(\bar{u}, \bar{v}) \leq d_H(\bar{u}, \bar{w}) + d_H(\bar{w}, \bar{v})$

Objevování a opravování chyb

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

Definice

Kód K *objevuje chybové slovo* $\bar{e}$, jestliže pro žádné kódové slovo $\bar{v} \in K$ není slovo $\bar{v} + \bar{e}$ kódové.

Tvrzení

Lineární kód K objevuje právě ta chybová slova, která nejsou kódová.

Objevování a opravování chyb

Definice

Kód K *objevuje t chyb*, jestliže objevuje každé chybové slovo váhy $\|\bar{e}\|_H \leq t$.

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:
$d_H(\bar{v}, \bar{v} + \bar{e}) < d_H(\bar{u}, \bar{v} + \bar{e})$ pro každé kódové slovo $\bar{u} \in K$, $\bar{u} \neq \bar{v}$.

Tvrzení

Kód opravuje (aspoň) t chyb právě, když objevuje (aspoň) $2t$ chyb.

Objevování a opravování chyb

Definice

Minimální vzdálenost kódu K je rovna nejmenší Hammingově vzdálenosti různých kódových slov:
$d_H(K) = \min\{d_H(\bar{u}, \bar{v}) \mid \bar{u}, \bar{v} \in K, \bar{u} \neq \bar{v}\}$.

Tvrzení

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

Objevování a opravování chyb

Tvrzení

Kód K má minimální vzdálenost $d_H(K) = d$ právě, když objevuje $d-1$ chyb a neobjevuje (libovolných) d chyb.
(Tedy kód opravuje $r = [\frac{d-1}{2}]$ chyb, ale více ne, resp. ne vždy).

Tvrzení

Nechť K je lineární $(n,k)-$kód nad $\mathbb{Z}_p$, pak platí nerovnost:

$$d_H(K) \leq n - k + 1$$

Aneb kód objevuje nejvýše $n-k$ chyb, tedy nejvýše tolik chyb, kolik má kontrolních znaků.

Standardní dekódování

Mějme lineární (n, k)-kód K nad $\mathbb{Z}_p$ s kontrolní matici $\mathbb{H}$.
Předpokládejme, že bylo posláno slovo $\bar{v} \in K$ a přijato slovo $\bar{w} = \bar{v} + \bar{e}$, kde $\bar{e}$ je *chybové slovo*.
Víme, že pokud $\mathbb{H}\,\bar{w}^T \neq \bar{o}^T$, tak nastala chyba ($\bar{e} \neq \bar{o}$).
Slovo $\bar{s}$, pro něž je $\mathbb{H}\,\bar{w}^T = \bar{s}^T$, se nazývá *syndrom* přijatého slova $\bar{w}$.

Tvrzení

Přijaté slovo má stejný syndrom jako jeho chybové slovo.

Standardní dekódování

Spočteme syndrom $\bar{s}$ přijatého slova $\bar{w}$ a pak hledáme chybové slovo $\bar{e}$ s co nejmenší vahou, které řeší soustavu $\mathbb{H}\,\bar{x}^T = \bar{s}^T$.

- Homogenní soustavu $\mathbb{H}\,\bar{x}^T = \bar{o}^T$ řeší právě všechna kódová slova $\bar{v} \in K$. Je-li $\bar{s} = \bar{o}$, pak $\bar{e}_o = \bar{o}$.
- Nehomogenní soustavu $\mathbb{H}\,\bar{x}^T = \bar{s}^T$ řeší právě všechna slova tvaru $\bar{w} + \bar{v}$, kde $\bar{w}$ je partikulární řešení a $\bar{v} \in K$.
- Vyberme z množiny všech řešení této nehomogenní soustavy jedno řešení s nejmenší Hammingovou vahou, označme je $\bar{e}_s$. (Je-li více řešení se stejnou nejmenší vahou, vezmene jedno z nich.)
- Pro každý syndrom $\bar{s}$ si zapišme do tabulky chybové slovo $\bar{e}_s$.

Standardní dekódování

- Takto vytvoříme tabulku chybových slov $\bar{e}_s$ s nejmenší vahou pro každý možný syndrom $\bar{s}$.
- Pro lineární (n, k)-kód K nad $\mathbb{Z}_p$ bude mít tabulka p^{n-k} řádků.

Standardní dekódování: Spočteme syndrom přijatého slova $\bar{w}$, podle tabulky zjistíme chybové slovo nejmenší váhy $\bar{e} = \bar{e}_s$. Opravíme na kódové slovo $\bar{v} = \bar{w} - \bar{e}$.

Tvrzení

Každé standardní dekódování je optimální co do počtu opravovaných chyb. Všechna slova, která mají jednoznačnou opravu (jediného nejbližšího souseda) opraví standardní dekódování správně.

Dekódování pomocí sloupců v $\mathbb{H}$

Mějme lineární (n, k)-kód K nad $\mathbb{Z}_p$ s kontrolní matici $\mathbb{H}$.
Bylo posláno kódové slovo $\bar{v}$ a přijato slovo $\bar{w} = \bar{v} + \bar{e}$.

Tvrzení

Přijaté slovo má stejný syndrom jako jeho chybové slovo:
$\mathbb{H}\,\bar{w}^T = \mathbb{H}\,\bar{e}^T = \bar{s}^T$
Syndrom je kombinací těch sloupců S_i kontrolní matice $\mathbb{H}$, jež odpovídají pozicím, kde je chyba: $\bar{s}^T = \sum_{e_i \neq 0} e_i S_i$

Pokud je ve slově $\bar{w}$ jedna chyba na i-té pozici, pak $\mathbb{H}\,\bar{w}^T = aS_i$.
Určíme-li jednoznačně a, S_i, můžeme chybu opravit:
$\bar{v} = \bar{w} - \bar{e}$, kde $e = (0 \ldots 0\, a\, 0 \ldots 0)$, $e_i = a$.

Dekódování pomocí sloupců v $\mathbb{H}$

Pozorování

- Lineární kód objevuje 1 chybu, pokud jeho kontrolní matice $\mathbb{H}$ neobsahuje nulový sloupec.
- Lineární kód opravuje 1 chybu (a objevuje 2 chyby), pokud žádný sloupec jeho kontrolní matice $\mathbb{H}$ není násobkem jiného sloupce v $\mathbb{H}$.

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.

Odtud znovu nerovnost $t \leq n - k$, kód objevuje nejvýše tolik chyb, kolik má kontrolních znaků.

Hammingovy kódy

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

Binární Hammingův kód s m kontrolními znaky

Pro daný počet kontrolních znaků m vytvoříme kontrolní matici $\mathbb{H}$ binárního Hammingova kódu:

- Chceme, aby kód opravoval jednu chybu, tudíž každé dva sloupce matice $\mathbb{H}$ musí být lineárně nezávislé. Nad $\mathbb{Z}_2$ jsou vektory lineárně nezávislé právě, když jsou nenulové a různé.
- Chceme co nejdelší kódová slova, tudíž $\mathbb{H}$ musí mít co nejvíce sloupců. $\mathbb{H}$ bude mít ve sloupcích právě všechny nenulové m-tice nad $\mathbb{Z}_2$.

Binární Hammingovy kódy

Informační poměr

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 $\frac{k}{n} = 1 - \frac{m}{2^m - 1}$ roste rychle k 1.
Pro $m = 3$ je $k : n = 4 : 7$, pro $m = 6$ je $k : n = 57 : 63$.

Snadné dekódování

Sloupce v $\mathbb{H}$ si lze představit jako binární rozvoje čísel 1 až $2^m - 1$. Seřadíme sloupce vzestupně, tedy $S_i = (i)_2$.

Opravování jedné chyby je pak snadné: Je-li syndrom přijatého slova je binárním rozvojem čísla i, pak je chyba na i-té pozici. Opravíme ji změnou i-tého znaku na opačný v $\mathbb{Z}_2$.

Binární Hammingovy kódy

Příklad

Pro $m = 3$ má kontrolní matice binárního Hammingova kódu tvar:

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

Přijaté slovo $\bar{w} = (1100001)$ má syndrom $\bar{s} = (100) = (4)_2$.
Dekódujeme na kódové slovo $\bar{v} = (1101001)$.

Binární Hammingovy kódy

Rozšířený Hammningův kód

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 $k = 2^m - 1 - m$.
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.
Rozšířený Hammingův kód opravuje jednu chybu, ale objevuje tři chyby.

Perfektní kódy

Definice

Lineární (n, k)-kód K nad $\mathbb{Z}_p$ je perfektní pro $t-$násobné opravy, jestliže pro každé slovo $\bar{w} \in \mathbb{Z}_p^n$ existuje právě jedno kódové slovo $\bar{v} \in K$ tak, že $d_H(\bar{v}, \bar{w}) \leq t$.
(Aneb kód opravuje t chyb a dokonce každé přijaté slovo lze opravit na kódové tak, že počet chyb je nejvýše t.)

Věta

Jediné netriviální perfektní binární kódy jsou:

- Hammingovy kódy pro jednonásobné chyby
- Opakovací kódy délky $2t + 1$ pro $t-$násobné chyby
- Golayův $(23, 12)$-kód pro trojnásobné chyby a kódy s ním ekvivalentní