NDMI028 Aplikace lineární algebry v kombinatorice
Handout No. 9

Samoopravné kódy, perfektní kódy, Lloydova věta
15. prosinec 2020

Samoopravné kódy

Definice (Samoopravný kód): Nechť A je konečná množina, budeme jí říkat *abeceda*. V dalším budeme značit $q = |A|$. Na množině A^n slov délky n definujeme vzdálenost (tzv. Hammingovu metriku) jako

$$d_H(x, y) = |\{i : x_i \neq y_i\}|.$$

Libovolnou podmnožinu $C \subseteq A^n$ nazýváme *kódem délky n nad abecedou o q symbolech*. Řekneme, že kód C *opravuje* t chyb, pokud

$$d_H(x, y) \geq 2t + 1$$

pro každá dvě různá slova $x, y \in C$.

Pozorování: Kód opravující t chyb lze využít ke komunikaci následovně. Na obou koncích komunikačního kanálu se před zahájením komunikace dohodneme, že budeme komunikovat výhradně kódovými slovy (příkladem takové dohody může být naprogramování kosmické sondy před vypuštěním do vesmíru). Během komunikace uvažujeme takto. Bylo-li vysláno slovo c, které se vlivem šumu v komunikačním kanálu nepodařilo správně přijmout na přijímači, přičemž došlo k nesprávné interpretaci v nejvýše t složkách vyslaného slova a bylo přijato slovo x, pak vyslané slovo c je v Hammingově metrice jediné nejbližší kódové slovo ke slovu x, tedy je možno jednoznačně určit, které slovo bylo vysláno.
Pozorování: Graf $\Gamma(n, q) = (A^n, \{xy : d_H(x, y) = 1\})$ je izomorfní n-té kartézské mocnině úplného grafu o q vrcholech. Přitom platí, že grafová vzdálenost v $\Gamma(n, q)$ je rovná Hammingově metrice. Kód C opravuje t chyb právě tehdy, když okolí kódových slov o poloměru t jsou po dvou disjunktní.

Tvrzení: Pokud kód C délky n nad abecedou o q symbolech opravuje t chyb, pak

$$|C| \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}. \tag{1}$$

Definice (Perfektní kód): Kód C délky n nad abecedou o q symbolech opravující t chyb se nazývá *t-perfektní*, pokud v (1) platí rovnost a $|C| > 1$.

Pozorování: Kód C délky n nad abecedou o q symbolech je t-perfektní právě tehdy, když okolí kódových slov o poloměru t tvoří rozklad množiny vrcholů grafu $\Gamma(n, q)$.

Tvrzení (Sphere packing condition): Pokud existuje t-perfektní kód délky n nad abecedou o $q = p^r$ symbolech pro prvočíslo p, potom

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i = q^k$$

pro nějaké přirozené číslo k.

Věta 1: Nechť $q = p^r$ pro prvočíslo p. Pak 1-perfektní kód délky n nad abecedou o q symbolech existuje tehdy a jen tehdy, když $n = \frac{q^k-1}{q-1}$ pro nějaké přirozené číslo k.
Důkaz: Pokud takový perfektní kód existuje, je podle Sphere packing condition $1+n(q-1) = q^k$ pro nějaké k, a tedy $n = \frac{q^k-1}{q-1}$.

Zkonstruovat kód takových parametrů je možno následovně. Nechť $n = \frac{q^k-1}{q-1}$ a nechť $H \in GF(q)^{k \times n}$ je matice, jejíž sloupce jsou po dvou lineárně nezávislé (tedy z každého jednodimenzionálního podprostoru prostoru $GF(q)^k$ vezmeme jeden nenulový vektor a použijeme jako jeden sloupec matice H). Potom $Ker(H) \subseteq GF(q)^n$ opravuje jednu chybu a přitom

$$|Ker(H)| = q^{dim(Ker(H))} = q^{n-k} = \frac{q^n}{q^k},$$

tedy kód $Ker(H)$ je 1-perfektní.

Existence perfektních kódů

Perfektní kódy jsou zajímavé tím, že skoro neexistují. V počátcích teorie kódování se zdálo, že perfektní kódy budou svatým grálem, neboť jsou nejefektivnější v tom smyslu, že dokážou opravit každé slovo (i když přesněji řečeno, každé slovo délky n se může dostat z nějakého kódového slova pomocí nejvýše t chyb). Kromě výše představených Hammingových kódů existují dva ojedinělé Golayovy kódy – 2-perfektní ternární kód délky 11 a 3-perfektní binární kód délky 23. Spojeným úsilím několika autorů (oddělených geograficky i v čase) se podařilo dokázat následující věty.

Věta 2: Je-li $q = p^r$ mocnina prvočísla, pak neexistují perfektní kódy jiných parametrů, než jsou parametry Hammingových a Golayových kódů (a opakovacího kódu s parametry $q = 2$, $n = 2t + 1$, který je považován za triviální).
Věta 3: Pokud q není mocnina prvočísla, pak neexistují žádné t-perfektní kódy opravující $t \geq 3$ chyb.

Kromě Sphere packing condition hraje v důkazech Vět 2 a 3 klíčovou roli Lloydova věta, jejíž souvislost s perfektními kódy se zdá na první pohled naprosto záhadnou.

Věta (Lloyd): Pokud existuje t-perfektní kód délky n nad abecedou s q symboly, pak polynom

$$L_t(x) = \sum_{j=0}^{t} (-1)^j (q-1)^{t-j} \binom{x-1}{j} \binom{n-x}{t-j}$$

má t různých kladných celočíselných kořenů menších než n.

Důkaz Lloydovy věty v obecném tvaru

Definice (Perfektní kódy v grafech): Množina vrcholů $C \subseteq V(G)$ v grafu G se nazývá t-perfektní kód v grafu G, pokud okolí kódových vrcholů o poloměru t tvoří rozklad množiny vrcholů $V(G)$ (a C má alespoň 2 vrcholy).
Definice (Vzdálenostně regulární grafy): Graf $G = (V, E)$ se nazývá *vzdálenostně regulární* pokud existují čísla s_{hij}, $h, i, j = 0, 1, \ldots, d$ (kde d je průměr grafu G), taková, že pro každé dva vrcholy $u, v \in V$ o vzdálenosti $d_G(u, v) = j$ platí

$$|\{w : d_G(u, w) = h, d_G(w, v) = i\}| = s_{hij}.$$

Pozorování: Každý vzdálenostně regulární graf je regulární, přičemž stupně vrcholů jsou $k = s_{110}$.
Pozorování: Je-li G vzdálenostně regulární, pak $s_{hij} = 0$ kdykoliv $|h - i| > j$.

Dohoda: Po zbytek této kapitoly předpokládáme, že pracujeme se vzdálenostně regulárním grafem $G = (V, E)$ průměru d. Přitom $k = s_{110}$, jak bylo zavedeno výše, a dále označíme $k_i = s_{ii0}$ pro $i = 2, 3, \ldots, d$.

Lemma 1: Počet sledů z_{mi} délky m mezi vrcholy o vzdálenosti i nezávisí na volbě těchto vrcholů.

Definice: Pro $i = 0, 1, \ldots, d$ označíme $A_i \in \{0, 1\}^{V \times V}$ matici vyjadřující vzdálenost i v grafu G, tedy

$$(A_i)_{uv} = \begin{cases} 1 \text{ pokud } d_G(uv) = i \\ 0 \text{ jinak.} \end{cases}$$

Definice: Nechť $C[x]$ značí množinu všech polynomů s komplexními koeficienty. Algebru $\mathcal{A}(G) = \{p(A) : p(x) \in C[x]\} \subseteq C^{V \times V}$ chápeme jako vektorový prostor nad tělesem C.

Lemma 2: Dimenze $\mathcal{A}(G)$ je $d + 1$ a matice $A_0, A_1, \ldots, A_d$ tvoří její bázi.

Definice: Pro matici $X \in \mathcal{A}(G)$ označme $\overline{X}$ matici endomorfismu $Y \to XY$ vůči bázi $A_0, A_1, \ldots, A_d$. Dále pišme $\hat{X} = \overline{X}^T$ a $\hat{\mathcal{A}}(G) = \{\hat{X} : X \in \mathcal{A}(G)\}$. Potom $\hat{}$ je izomorfismus algeber $\mathcal{A}(G)$ a $\hat{\mathcal{A}}(G)$. Pro stručnost píšeme $B_h = \hat{A}_h$, a speciálně $B = B_1$.

Lemma 3: Pro každé h, i, j je $(B_h)_{ij} = s_{hij}$.

Lemma 4: Matice B je tridiagonální a součet prvků v každém sloupci je roven k.

Definice: Rekurzivně definujeme polynomy $v_i(\lambda) \in C[\lambda]$, pro $i = 0, 1, \ldots, d$, následovně

$$v_0(\lambda) = 1$$

$$v_1(\lambda) = \lambda$$

$$s_{1,i,i-1}v_{i-1}(\lambda) + (s_{1,i,i} - \lambda)v_i(\lambda) + s_{1,i,i+1}v_{i+1}(\lambda) = 0$$

pro $i = 1, 2, \ldots, d-1$.

Lemma 5: Nechť $\lambda_0, \lambda_1, \ldots, \lambda_d$ jsou vlastní čísla matice B. Protože B je tridiagonální a prvky podél hlavní diagonály jsou všechny nenulové, jsou vlastní čísla matice B po dvou různá. Číslo k je vlastní číslo, nechť nadále $\lambda_0 = k$. Potom

$$v_0(\lambda) + v_1(\lambda) + \ldots + v_d(\lambda) = c(\lambda - \lambda_1) \cdots (\lambda - \lambda_d)$$

.

Lemma 6: Pro každé $i = 0, 1, \ldots, d$ platí

$$k_i = v_i(k)$$

$$A_i = v_i(A)$$

$$B_i = v_i(B).$$

Definice: Pro libovolný vrchol $z \in V$ zavedeme matici $T_z \in \{0, 1\}^{(d+1)\times n}$ takto

$$(T_z)_{iu} = \begin{cases} 1 & \text{pokud } d_G(u, z) = i \\ 0 & \text{jinak.} \end{cases}$$

Lemma 7: Pro každou matici $X \in \mathcal{A}(G)$ a pro každý vrchol $z \in V$ platí

$$T_z X = \hat{X} T.$$

Definice: Pro $i = 0, 1, \ldots, d$ zavedeme polynomy

$$x_i(\lambda) = v_0(\lambda) + v_1(\lambda) + \ldots + v_i(\lambda)$$

a označíme matici

$$S_i = x_i(A) = A_0 + A_1 + \ldots + A_i.$$

Lemma 8: Je-li $c \in \{0,1\}^V$ charakteristický vektor t-perfektního kódu v grafu G, pak $S_t c = \mathbf{1}$.

Lemma 9: Pokud v grafu G existuje t-perfektní kód, pak $\dim Ker(\hat{S}_t) \geq t$.

Důkaz: Nechť C je t-perfektní kód v G a nechť c je jeho charakteristický vektor. Zvolme vrcholy $z_0, z_1, \ldots, z_t$ tak, aby $z_0 \in C$ a $d_G(z_0, z_i) = i$ pro $i = 1, 2, \ldots, t$.

Vektory $T_{z_i} c, i = 0, 1, , \ldots, t$ jsou lineárně nezávislé, neboť

$$(T_{z_i} c)_j = \begin{cases} 1 & \text{pro } j = i \\ 0 & \text{jinak.} \end{cases}$$

Dále pro každé $i = 0, 1, \ldots, t$ je

$$\hat{S}_t T_{z_i} c = T_{z_i} S_t c = T_{z_i} \mathbf{1} = (k_0, k_1, \ldots, k_d)^T,$$

a proto vektory

$$w_i = (T_{z_i} - T_{z_0})c, i = 1, 2, \ldots, t$$

jsou lineárně nezávislé vektory patřící do $Ker(\hat{S}_t)$.

Věta 4 (Biggs): Pokud G obsahuje t-perfektní kód, potom polynom $x_t(\lambda)$ beze zbytku dělí polynom $x_d(\lambda)$. Jinak řečeno, kořeny polynomu $x_t(\lambda)$ jsou navzájem různá vlastní čísla matice B.

Důkaz: Matice B má $d + 1$ různých vlastních čísel $\lambda_0 = k, \lambda_1, \ldots, \lambda_d$, přičemž

$$x_d(\lambda) = c(\lambda - \lambda_1) \cdots (\lambda - \lambda_d).$$

Matice $\hat{S}_t = x_t(B)$ má vlastní čísla $x_t(\lambda_i), i = 0, 1, \ldots, d$. Protože 0 je alespoň t-násobné vlastní číslo matice $\hat{S}_t$, má polynom $x_t(\lambda)$ alespoň t kořenů mezi čísly $\lambda_1, \lambda_2, \ldots, \lambda_d$. Protože $x_t(\lambda)$ je polynom stupně t, jsou všechny jeho kořeny mezi kořeny polynomu $x_d(\lambda)$.

Důkaz Lloydovy věty

Perfektní kódy v Hammingově metrice nad abecedou s q symboly jsou perfektní kódy v grafu K_q^n. Tento graf je vzdálenostně regulární s parametry

$$d = n$$

$$s_{1,i,i-1} = (n-i+1)(q-1)$$
$$s_{1,i,i} = i(q-2)$$
$$s_{1,i,i+1} = i+1.$$

Pokud rekurzi

$$(n-i+1)(q-1)v_{i-1}(\lambda) + (i(q-2)-\lambda)v_i(\lambda) + (i+1)v_{i+1}(\lambda) = 0 \tag{2}$$

prodloužíme pro $i \to \infty$ a zavedeme vytvořující funkci

$$V(\lambda, z) = \sum_{i=0}^{\infty} v_i(\lambda) z^i,$$

dostaneme po zderivování podle z

$$\frac{dV}{dz} = \sum_{i=0}^{\infty} i v_i(\lambda) z^{i-1} = \sum_{i=0}^{\infty} (i+1) v_{i+1}(\lambda) z^i$$

a po vynásobení (2) faktorem z a sečtení

$$(1 + z(q-2) - z^2(q-1))\frac{dV}{dz} = (\lambda - n(q-1)z)V(\lambda, z).$$

Po integraci per partes pak

$$\ln V + C = \int \frac{dV}{V} = \int \frac{\lambda - n(q-1)z}{(1+z(q-1))(1-z)} dz = \frac{n+\lambda}{q}\ln(1+z(q-1)) + \frac{n(q-1)-\lambda}{q}\ln(1-z),$$

přičemž integrační konstanta $C = 0$, protože $V(\lambda, 0) = 1$. Po odlogaritmování a substituci $y = n - \frac{n+\lambda}{q}$ dostaneme

$$V(\lambda, z) = (1+z(q-1))^{n-y}(1-z)^y.$$

Podobně prodloužíme definici $x_i(\lambda) = \sum_{j=0}^{t} v_i(\lambda)$ pro $i \to \infty$ a zavedeme

$$X(\lambda, z) = \sum_{i=0}^{\infty} x_i(\lambda) z^i.$$

Potom

$$X(\lambda, z) = \sum_{i=0}^{\infty} (\sum_{j=0}^{i} v_j(\lambda)) z^i = \sum_{j=0}^{\infty} \sum_{i=j}^{\infty} v_j(\lambda) z^i = \sum_{j=0}^{\infty} v_j(\lambda) \frac{z^j}{1-z} =$$

$$= \frac{1}{1-z} V(\lambda, z) = (1 + z(q-1))^{n-y} (1-z)^{y-1}.$$

Vidíme, že pro každé $y = 1, 2, \ldots, n$ je $X(\lambda, z)$ polynom stupně $n-1$ v z, a tedy pro každé $y = 1, 2, \ldots, n$ je $x_n(\lambda) = x_n(n(q-1) - qy) = 0$. Protože $x_n(n(q-1) - qy)$ je nenulový polynom stupně n v y, jsou toto všechny jeho kořeny. Biggsova věta pak říká, že obsahuje-li K_q^n t-perfektní kód, jsou všechny kořeny polynomu $x_t(\lambda)$ obsaženy mezi $\lambda = n(q-1) - qy, y = 1, 2, \ldots, n$, a tedy

$$x_t(n(q-1) - qy) = \sum_{j=0}^{t} (-1)^j \binom{y-1}{j} \binom{n-y}{t-j} (q-1)^{t-j}$$

má všechny kořeny mezi $y = 1, 2, \ldots, n$.