SEMINARSKA NALOGA
Shannonova kapaciteta

Peter Pešec
Blaž Knep
Jože Salcman

6.maj 2003

Leta 1956 je Claude Shannon, izumitelj informacijske teorije, postavil naslednje zanimivo vprašanje:
Predpostavimo, da želimo poslati sporočilo po kanalu, kjer se lahko nekateri simboli pomešajo, sprejemniku. Kaj je največja stopnja prenosa, da prejemnik še lahko razbere originalno sporočilo brez napak?

Pa poglejmo, kaj je Shannon mislil s kanalom in stopnjo prenosa:
Imamo množico simbolov V in sporočilo je le zaporedje simbolov iz V. Kanal oblikujemo kot graf $G = (V, E)$, kjer je V množica simbolov in E množica povezav med simboli, ki se lahko pomešajo.

Npr.:
V vsakdanji telefoniji povežemo simbola P in B s povezavo, ker ju prejemnik nenujnoo loči.

Graf G imenujemo graf zmešnjav.

Pet cikel C_5 bo igral ključno vlogo v naši diskusiji.
V našem primeru se lahko 1 in 2 pomešata ne pa 1 in 3!
Seveda bi si želeli komunicirati z vsemi petimi simboli, ker pa ne želimo napak (če pošiljamo posamezne simbole) uporabimo le po en simbol iz vsakega para, ki se lahko pomešajo, zato lahko v C_5 uporabimo le 2 simbola (katerakoli, ki nista povezana).
V jeziku informacijske teorijeto pomeni, da smo v C_5 dosegli stopnjo prenosa $\log_2 2$ namesto $\log_2 5$. Jasno je, da v tem modelu za graf $G = (V, E)$, lahko v najboljšem primeru pošljemo iz maksimalne neodvisne podmnožice grafa G, da bo stopnja prenosa (pri pošiljanju posameznih simbolov) $\log_2 \alpha(G)$, pri čemer je $\alpha(G)$ neodvisnostno število.

Poglejmo si, če lahko povečamo stopnjo prenosa z uporabo daljših nizov namesto posameznih simbolov.
Predpostavimo, da želimo poslati niz dolžine 2. Niza u_1u_2 ter v_1v_2 lahko pomešamo le v primeru, ko velja en izmed pogojev:

1.) $u_1 = v_1$ in u_2 se lahko zamenja z v_2
2.) $u_2 = v_2$ in u_1 se lahko zamenja z v_1
3.) $u_1 \neq v_1$ se lahko zamenjata in $u_2 \neq v_2$ se lahko zamenjata

V teoriji grafov : $G_1 \times G_2 \quad , G_1 = (V_1, E_1), G_2 = (V_2, E_2)$

$G_1 \times G_2 = \{(u_1, u_2)|u_1 \in V_1, u_2 \in V_2\}$, pri čemer sta $(u_1, u_2) \neq (v_1, u_2)$ povezana z natanko eno povezavo natanko takrat, ko velja $u_i = v_i$ ali $u_i v_i \in E, i = 1, 2$.

Graf zmešnjav nizov dolžine 2 je $G^2 = G \times G$, produkt grafa samim s seboj. Stopnja prenosa nizov dolžine 2 po simbolu je

$$\frac{\log_2 \alpha(G^2)}{2} = log_2 \sqrt{\alpha(G^2)}$$

Seveda lahko uporabljamo nize poljubne dolžine n. n-ti graf zmešnjave $G^n = G \times G \times G \times ... \times G$ vsebuje $V^n = \{(u_1, u_2, ..., u_n)|u_i \in V\}$, pri čemer je $(u_1, ..., u_n) \neq (v_1, ..., v_n)$ povezan s povezavo če $u_i = v_i$ ali $u_i v_i \in E$ za $i = 1, ..., n$
Stopnja prenosa po simbolu nizov dolžine n je

$$\frac{\log_2 \alpha(G^n)}{n} = log_2 \sqrt[n]{\alpha(G^n)}$$

Kaj lahko povemo o $\alpha(G^n)$? [neodvisnostno število grafa G^n]
Prvo opažanje:
Če je $U \subseteq V$ največja neodvisna podmnožica v G,
potem je $|U| = \alpha \quad \Rightarrow \quad \alpha^n$ v G^n oblike $(u_1, ..., u_n), u_i \in V$ za vse i neodvisna podmnožica v G^n.
Ker je $\alpha(G^n) \geq \alpha(G)^n \quad \Rightarrow \quad \sqrt[n]{\alpha(G^n)} \geq \alpha(G)$, pomeni da nikoli ne zmanjšamo stopnje prenosa z uporabo daljših nizov namesto posameznih simbolov.

To je osnovna ideja teorije kodiranja:
z odkodiranjem simbolov v daljše nize lahko naredimo komuniciranje bolj učinkovito.

Če zanemarimo logaritem, potemtakem pridemo do Shannonove osnovne definicije:
Shannon-ova kapaciteta grafa G je podana z

$$\Theta(G) = sup_{n \geq 1} \sqrt[n]{\alpha(G^n)}$$

in Shannonov problem je bil oceniti $\Theta(G)$ in konkreten $\Theta(C_5)$

Pa si poglejmo C_5. Kot že vemo je

$$\alpha(C_5) = 2 \leq \Theta(C_5)$$

Če gledamo na 5-cikel kot prej, ali pa kot produkt $C_5 \times C_5$
Vidimo, da je množica $\{(1,1),(2,3),(3,5),(4,2),(5,4)\}$ neodvisna v C_5^2.
Torej imamo

$$\alpha(C_5^2) \geq 5$$

Ker neodvisna množica lahko vsebuje le dve točki iz vsake dve zaporedni vrstici, vidimo, da je

$$\alpha(C_5^2) = 5$$

Zato, z uporabo nizov dolžine 2 smo povečali spodnjo mejo na

$$\Theta(C_5) \geq \sqrt{5}$$

Nimamo pa zgornje omejitve. Da bi dobili takšno mejo se ponovno oprimimo Shannonove prvotne ideje. Najprej potrebujemo dualno definicijo neodvisne množice.
Spomnimo se, da je podmnožica $C \subseteq V$ **klika** natanko tedaj, če sta vsaki dve točki v C povezani.
Zato so točke trivialne klike dolžine 1, povezave z robnima točkama klike dolžine 2, trikotniki klike dolžine 3, itd.

Naj bo $\mathcal{C}$ množica vseh klik v G in naj bo $\mathbf{x}= (x_v : v \in V)$ verjetnostna porazdelitev:

$$(x_v \geq 0, \sum_{v \in V} x_v = 1)$$

Vsaki porazdelitvi $\mathbf{x}$ priredimo maksimalno vrednost klike

$$\lambda(x) = \max_{C \in \mathcal{C}} \sum_{v \in C} x_v$$

ter

$$\lambda(G) = \min_x \lambda(x) = \min_x \max_{C \in \mathcal{C}} \sum_{v \in C} x_v$$

Če smo natannčni, bi morali namesto min pisati inf , vendar je $\lambda(x)$ zvezna funkcija na kompaktni množici vseh porazdelitev.

Naj bo $U \subseteq V$ maksimalna neodvisna podmnožica V. Tedaj je $|U| = \alpha(G)$ Tej množici U priredimo verjetnostno porazdelitev

$$x_U = (x_v : v \in V),$$

pri čemer je

$$x_v = \begin{cases} \frac{1}{\alpha} & ; v \in U \\ 0 & ; sicer \end{cases}$$

Ker vsaka klika vsebuje največ eno točko iz U, vidimo, da je

$$\lambda(x_U) = \frac{1}{\alpha}$$

Po definiciji $\lambda(G)$ velja

$$\lambda(G) \leq \lambda(x_U) = \frac{1}{\alpha(G)}$$

oziroma

$$\alpha(G) \leq \lambda(G)^{-1}$$

Shannon je ugotovil, da je $\lambda(G)^{-1}$ zgornja meja za vse izraze $\sqrt[n]{\alpha(G^n)}$, pri čemer je $n \in \mathbb{N}$, torej tudi za $\Theta(G)$.
Da bomo to dokazali, zadostuje, če dokažemo, da za vsaka grafa H, G velja $\lambda(G \times H) = \lambda(G) \cdot \lambda(H)$, ker od tod sledi, da je $\lambda(G^n) = \lambda(G)^n$ in zato $\alpha(G^n) \leq \lambda(G^n)^{-1} = \lambda(G)^{-n}$.

Dokaz:
Uporabili bomo izrek o dualnosti iz teorije linearnega programiranja in dobimo

$$\lambda(G) = \min_x \max_{C \in \mathcal{C}} \sum_{v \in C} x_v = \max_y \min_{v \in V} \sum_{C \ni v} y_C$$

kjer desna stran teče po vseh verjetnostnih porazdelitvah $y = (y_C : C \in \mathcal{C})$.
Vzemimo $G \times H$ in naj bosta x in x' porazdelitvi v katerih λ doseže minimum.

$\lambda(x) = \lambda(G)$

$\lambda(x') = \lambda(H)$

V množici točk grafa $G \times H$ definiramo vrednost $z_{(u,v)} = x_u x'_v$ točki (u, v).
Ker

$$\sum_{(u,v)} z_{(u,v)} = \sum_u x_u \cdot \sum_v x'_v = 1$$

Opazimo, da je maksimalna klika v $G \times H$ oblike $C \times D = \{(u,v) | u \in C, v \in D\}$, kjer je C klika v G in D klika v H.
Zato je

$$\lambda(G \times H) \leq \lambda(z) = \max_{C \times D} \sum_{(u,v) \in C \times D} z_{(u,v)} = \max_{C \times D} \sum_{u \in C} x_u \cdot \sum_{v \in D} x'_v = \lambda(G) \cdot \lambda(H)$$

Obratno neenakost se pokaže z uporabo izreka o dualnosti. $\square$

Če povežemo: $\Theta(G) \leq \lambda(G)^{-1}$ za vsak graf G.

Pa si poglejmo za C_5 oziroma splošneje za C_m:

Z uporabo enakomerne porazdelitve $(\frac{1}{m}, ..., \frac{1}{m})$ dobimo $\lambda(C_m) \leq \frac{2}{m}$.
Podobno če vzamemo $\frac{1}{m}$ za povezave, in 0 za točke, ugotovimo, da je $\lambda(C_m) \geq \frac{2}{m}$ po izreku dualnosti.
Od to sledi, da je $\lambda(C_m) = \frac{2}{m}$
Zato je $\Theta(C_m) \leq \frac{m}{2}$ za vse m.

Za m je sodo število je $\alpha(C_m) = \frac{m}{2}$ (vsaka druga točka)
Zato je $\Theta(C_m) = \frac{m}{2}$

Za lihe m -je pa je $\alpha(C_m) = \frac{m-1}{2}$

C_3:
C_3 je klika, zato je tudi C_3^n klika.
Zato $\alpha(C_3) = \Theta(C_3) = 1$

C_5:

$$\sqrt{5} \leq \Theta(C_5) \leq \frac{5}{2}$$

Z uporabo linearnega programiranja in drugih idej je Shannon bil sposoben izračunati $\Theta(G)$ za mnoge grafe G, še posebej za tiste s 5 ali manj točkami , z eno samo izjemo: C_5, za katerega ni našel boljše ocene za $\Theta(C_5)$!
Tako so stvari stale več kot 20 let, dokler ni Laszlo Lovasz ni izračunal, da je $\Theta(C_5) = \sqrt{5}$.

Na prvi pogled zelo težek kombinatorični problem je bil enostavno in elegantno rešen. Lovasz-ova glavna ideja bila predstaviti točke grafa z realnimi vektorji dolžine 1, tako da sta vsaka dva vektorja, ki pripadata dvema nepovezanima točkama v grafu G, pravokotna. Takšno predstavitev imenujemo ortonormirana predstavitev grafa G. Očitno taka predstavitev vedno obstaja. Lahko vzamemo bazne vektorje dimenzije $m = |V|$.

Za cikel C_5 vidimo, da je ortonormirana predstavitev v $\mathbb{R}^3$ kot dežnik s pet rebri, $v_1, ..., v_5$, enotske dolžine.
Z odpiranjem pridemo do pozicije, kjer je kot med dvema nesosednima rebroma previ.
Izkaže se:

$$\Theta(C_5) \leq \frac{1}{h^2},$$

kjer je h razdalja vrha do S. Računsko se izkaže, da je $h^2 = \frac{1}{\sqrt{5}}$ in zato

$$\Theta(C_5) \leq \sqrt{5},$$

od koder sledi

$$\Theta(C_5) = \sqrt{5}.$$

Naj bo $G = G(V, E)$ poljuben graf z m točkami in naj bo množica vektorjev $T = \{v^{(1)}, ..., v^{(m)}\}$ ortonormalna reprezentacija grafa G. To pomeni, da za vsak $i = 1, ..., m$ velja $||v^{(i)}|| = 1$ in $\langle v^{(i)}, v^{(j)} \rangle = 0$ tedaj in samo tedaj, ko točki i in j na grafu G nista sosednji. Označimo z $u := \frac{1}{m}(v^{(1)} + ... + v^{(m)})$. Očitno je skalarni produkt

$$\langle v^{(i)}, u \rangle := \sigma_T$$

različen od nič in za vsak i enak. Definirajmo porazdelitev kot vektor

$$\mathbf{x} := (x_1, ..., x_m)$$

za katerega velja $x_i \geq 0$ in je vsota njegovih koordinat enaka 1. Dalje definirajmo $\mu(\mathbf{x}) := ||x_1 v^{(1)} + ... + x_m v^{(m)}||^2$ in končno definirajmo

$$\mu_T(G) := inf_{\mathbf{x}}\ \mu(\mathbf{x})$$

infimum vrednosti $\mu(\mathbf{x})$ po vseh porazdelitvah $\mathbf{x}$. Naj bo U maksimalna neodvisna množica točk grafa G. Torej je $|U| = \alpha(G)$, kjer je $\alpha(G)$ neodvisnostno število grafa G. Označimo z

$$\mathbf{x}_U = (x_1, ..., x_m)$$

kjer je $x_i = \frac{1}{\alpha(G)}$, če je $x_i \in U$ in 0 sicer. Očitno je $\mathbf{x}_U$ porazdelitev (vse koordinate so nenegativne in vsota vseh je ravno 1). Sledi $\mu_T(G) \leq \mu(\mathbf{x}_U)$, saj je $\mu_T(G)$ infimum po vseh porazdelitvah, dalje velja (upoštevamo $||a|| = \langle a, a \rangle$, bilinearnost skalarnega produkta, da $||v^{(i)}|| = 1$ in $\langle v^{(i)}, v^{(j)} \rangle = 0$, če točki i, j nista sosednji ter U je neodvisna podmnožica grafa G zato ne vsebuje dveh sosednjih točk grafa G- ena od koordinat x_i in x_{i+1} je 0)

$$\mu(\mathbf{x}_U) = ||x_1 v^{(1)} + ... + x_m v^{(m)}||^2 = \langle x_1 v^{(1)} + ... + x_m v^{(m)}, x_1 v^{(1)} + ... + x_m v^{(m)} \rangle =$$

$$= x_1^2 + ... + x_m^2 = \alpha(G) \frac{1}{(\alpha(G))^2} = \frac{1}{\alpha(G)}$$

glede na to, da je le $\alpha(G)$ neničelnih koordinat. Ugotovili smo torej:

$$\alpha(G) \leq \frac{1}{\mu_T(G)}$$

V naslednjem koraku si oglejmo naslednji izraz, kjer je $\mathbf{x} = (x_1, ..., x_m)$ poljubna porazdelitev in uporabimo Cauchy-Schwarzovo neenakost:

$$\langle x_1 v^{(1)} + ... + x_m v^{(m)}, u \rangle^2 \leq ||x_1 v^{(1)} + ... + x_m v^{(m)}||^2 ||u||^2 = \mu(\mathbf{x}) ||u||^2$$

Oglejmo si še

$$\langle x_1 v^{(1)} + ... + x_m v^{(m)}, u\rangle = \sigma_T(x_1 + ... + x_m) = \sigma_T$$

Tukaj smo upoštevali lastnosti skalarnega produkta in da je $\mathbf{x}$ porazdelitev (vsota koordinat je 1). Posebej za enakomerno porazdelitev $\mathbf{x}_E = (\frac{1}{m}, ..., \frac{1}{m})$ dobimo

$$\sigma_T = \langle \frac{1}{m} v^{(1)} + ... + \frac{1}{m} v^{(m)}, u\rangle = \langle u, u\rangle = ||u||^2$$

Število σ_T je torej enako kvadratu norme vektorja u, ki je za dano repretentacijo T grafa G konstantno. Iz zgornjih dveh identitet (v prvi identiteti namesto $||u||^2$ pišimo σ_T) dobimo $\sigma_T^2 \leq \mu(\mathbf{x})\sigma_T$, oziroma $\sigma_T \leq \mu(\mathbf{x})$. To velja za vsako porazdelitev tudi za infumum. Tako smo prišli do $\sigma_T \leq \mu_T(G)$. Če za $\mathbf{x}$ spet vzamemo enakomerno porazdelitev $\mathbf{x}_E$ velja tudi

$$\mu_T(G) \leq \mu(\mathbf{x}_E) = ||\frac{1}{m}(v^{(1)} + ... + v^{(m)})||^2 = ||u||^2 = \sigma_T$$

Končno smo izpeljali $\mu_T(G) = \sigma_T$ oziroma

$$\alpha(G) \leq \frac{1}{\sigma_T}$$

Brez dokaza navedimo tehničen rezultat: Za vsak $x \in \mathbb{N}$ velja $\alpha(G^n) \leq \frac{1}{\sigma_T^n}$ oziroma

$$(\alpha(G^n))^{\frac{1}{n}} \leq \frac{1}{\sigma_T}$$

Od tu zlahka sledi osnovni *Lovász*-ev izrek:

$$\Theta(G) := sup_{n\in\mathbb{N}}\ \alpha(G^n))^{\frac{1}{n}} \leq \frac{1}{\sigma_T}$$

pri čemer (spomnimo se) velja $\sigma_T = \langle v^{(i)}, u\rangle$ in so vektorji $v^{(i)}$ ortonormalna reprezentacija grafa G, za vektor u pa velja $u = \frac{1}{m}(v^{(1)} + ... + v^{(m)})$.

Oglejmo si zdaj primer ko $G = C_5$. Za graf C_5 definirajmo matriko $A = (a_{i,j})$, za katero velja:

$$a_{i,j} := \begin{cases} 1 & ; v_i v_j \in E \\ 0 & ; sicer \end{cases}$$

Dobimo realno simetrično matriko dimenzije 5×5 z samimi ničlami na glavni diagonali. Iz linearne algebre vemo, da ima taka simetrična matrika 5 realnih lastnih vrednosti $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4 \geq \lambda_5$ in da je njihova vsota enaka vsoti členov na diagonali, to je v našem primeru 0. Zato je vsaj ena lastna vrednost naše matrike negativna (možnost, da so vse lastne vrednosti enake 0 odpade, saj je naša matrika neničelna).

Izračunajmo lastne vrednosti matrike A. Označimo z $\xi = e^{\frac{2\pi i}{5}} = \cos(\frac{2k\pi}{5}) + i\sin(\frac{2k\pi}{5})$ rešitev enačbe $x^5 = 1$. Potem so vse nadaljne rešitve ξ^k, kjer $0 \leq k \leq 4$. Za vsak $0 \leq k \leq 4$ velja:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \xi^k \\ \xi^{2k} \\ \xi^{3k} \\ \xi^{4k} \end{pmatrix} = \begin{pmatrix} \xi^k + \xi^{-k} \\ 1 + \xi^{2k} \\ \xi^k + \xi^{3k} \\ \xi^{2k} + \xi^{-k} \\ 1 + \xi^{3k} \end{pmatrix} = (\xi^k + \xi^{-k}) \begin{pmatrix} 1 \\ \xi^k \\ \xi^{2k} \\ \xi^{3k} \\ \xi^{4k} \end{pmatrix}$$

Ugotovili smo, da je za vsak $0 \leq k \leq 4$, vektor $(1, \xi^k, \xi^{2k}, \xi^{3k}, \xi^{4k})^T$ lastni vektor za lastno vrednost $\xi^k + \xi^{-k}$. Za vsak k dobimo lastno vrednost in pripadajoči lastni vektor. Očitno za $k = 2, 3$ dobimo najmanjšo lastno vrednost, to je $2\cos(\frac{4\pi}{5}) = -2\cos\frac{\pi}{5}$.

k	$\xi^k + \xi^{-k}$
$k = 0$	2
$k = 1$	$2\cos(\frac{2\pi}{5})$
$k = 2$	$2\cos(\frac{4\pi}{5})$
$k = 3$	$2\cos(\frac{6\pi}{5})$
$k = 4$	$2\cos(\frac{8\pi}{5})$

Tabela 1: Lastne vrednosti matrike A

Označimo s $p = |\lambda_5|$ absolutno vrednost najmanjše lastne vrednosti in si oglejmo matriko:

$$M := I + \frac{1}{p}A$$

kjer je I identična matrika.
Očitno so $1 + \frac{\lambda_1}{p} \geq 1 + \frac{\lambda_2}{p} \geq 1 + \frac{\lambda_3}{p} \geq 1 + \frac{\lambda_4}{p} \geq 1 + \frac{\lambda_5}{p} = 0$ vse lastne vrednosti

za M. Matrika $M = (m_{i,j})$ je realna simetrična matrika z nenegativnimi realnimi lastnimi vrednostmi velikosti 5×5. Iz linearne algebre vemo, da za takšno matriko obstajajo vektorji $v^{(1)}, v^{(2)}, v^{(3)}, v^{(4)}, v^{(5)} \in \mathbb{R}^s$, kjer je $s = rank(M)$, da je člen

$$m_{i,j} = \langle v^{(i)}, v^{(j)} \rangle$$

kjer velja $1 \leq i, j \leq 5$
Za $M := I + \frac{1}{p}A$ ugotovimo da je

$$\langle v^{(i)}, v^{(i)} \rangle = m_{i,i} = 1$$

in za $i \neq j$ velja

$$\langle v^{(i)}, v^{(j)} \rangle = \frac{1}{p} a_{i,j}$$

Ker je $a_{i,j} = 0$ natanko tedaj ko točki i in j nista sosednji predstavljajo vektorji $v^{(i)}$ ortonormalno reprezentacijo točk grafa.
Uporabimo ta spoznanja na naši matriki M. Zapišimo matriko M:

$$M = \begin{pmatrix} 1 & p^{-1} & 0 & 0 & p^{-1} \\ p^{-1} & 1 & p^{-1} & 0 & 0 \\ 0 & p^{-1} & 1 & p^{-1} & 0 \\ 0 & 0 & p^{-1} & 1 & p^{-1} \\ p^{-1} & 0 & 0 & p^{-1} & 1 \end{pmatrix}$$

Za vsak i velja:

$$\langle v^{(i)}, v^{(1)} + ... + v^{(5)} \rangle = \langle v^{(i)}, v^{(1)} \rangle + ... + \langle v^{(i)}, v^{(5)} \rangle$$

Zadnji izraz je ravno vsota členov v i-ti vrstici matrike M to pa je $1 + \frac{2}{p}$. Zdaj lahko izračunamo naš $\langle v^{(i)}, u \rangle := \sigma_T$, kjer je $u = \frac{1}{5}(v^{(1)} + ... + v^{(5)})$. Upoštevamo lastnosti skalarnega produkta in ugotovimo

$$\sigma_T := \langle v^{(i)}, u \rangle = \frac{1}{5}(1 + \frac{2}{p})$$

Če spet upoštevamo glavni izrek dobimo

$$\Theta(C_5) \leq \frac{1}{\sigma_T} = \frac{1}{\frac{1}{5}(1 + \frac{2}{p})} = 5\frac{1}{1 + \frac{2}{p}}$$

Če za p vstavimo $2\cos(\frac{\pi}{5})$ dobimo

$$\Theta(C_5) \leq \frac{5}{1 + (\cos\frac{\pi}{5})^{-1}}$$