NYILATKOZAT

Név: Matolcsi Dávid

ELTE Természettudományi Kar, szak: Matematika BSc

NEPTUN azonosító: O20K87

Szakdolgozat címe:
Változatok a gráfkapacitás fogalmára

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2022. 05. 30.

Matolcsi Dávid

a hallgató aláírása

Eötvös Loránd Tudományegyetem
Természettudományi Kar

Matolcsi Dávid
Matematika BSc

Változatok a gráfkapacitás fogalmára

Szakdolgozat

Külső témavezető: Simonyi Gábor egyetemi tanár (BME)
Belső témavezető: Frenkel Péter egyetemi docens
Algebra és Számelmélet Tanszék

Budapest, 2022

Köszönetnyilvánítás

Elsősorban köszönettel tartozom Simonyi Gábor témavezetőmnek, aki érdekes forrásokkal és kérdésekkel látott el, és konzultációink során tanácsot adott, hogy melyik témákat érdemes feldolgozni, illetve magyarázataival segítette egyes részek megértését. Köszönöm továbbá rendkívül alapos lektorálását, melynek során sok kisebb hibát észrevett és segített kijavítani a dolgozatomban.

Köszönet illeti Frenkel Péter tanár urat is, aki elvállalta, hogy az intézményen belüli témavezetőm lesz. Köszönöm Kiss Melindának, hogy kikölcsönözte nekem a Rényi Intézet könyvtárából Csiszár és Körner Information Theory könyvének új kiadását, amely könyv dolgozatom legfontosabb forrása. Köszönöm Szabó Kristófnak a dolgozat megíráshoz nyújott technikai segítséget, és Imolay Andrásnak a Tutte-tétel bizonyításának leírásához tett javaslatait.

Ezen kívül általános köszönettel tartozom minden egyetemi, közép- és általános iskolai matematikatanáromnak, a szüleimnek, és mindenkinek, aki valamilyen formában matematikát tanított nekem, hogy megadták azt a háttértudást, amely nélkül nem érthettem volna meg az itt feldolgozott matematikai eredményeket.

Tartalomjegyzék

1. Bevezetés

Szakdolgozatom az információelmélet kérdéseivel foglalkozik, azon belül is elsősorban a zéró-hiba információküldés kérdéskörével.

Legfőbb forrásom Csziszár Imre és Körner János Information Theory című, a témában meghatározó könyvének második kiadása volt [5].

Dolgozatom kezdetén bemutatok néhány, az információelméletben alapvető fogalmat és állítást, és röviden szót ejtek az ε-hibájú forrás- és csatorna-kódolásról. Később a Kapacitás típusokon belül alfejezetben szintén mélyebben tárgyalok egy, az információelméletben általánosan használt fogalmat. Ezek, a téma általános információelméleti hátterét bemutató részek elsősorban a könyv 1., 2. és 6. fejezeteinek feldolgozásából születtek.

Dolgozatom legnagyobb része a zéró-hiba információküldés kérdéskörét járja körül, ehhez legfőbb forrásom Csiszár és Körner könyvének ezzel a témával foglalkozó 11. fejezete. Dolgozatomban bemutatok néhány, a tételek jelentésére rámutató példát, és kapcsolódó tételt, ezek a 11. fejezethez tartozó feladatként szerepelnek a könyvben bizonyítás nélkül, itt azonban bizonyítással együtt prezentálom őket.

Az utolsó fejezet a Witsenhausen-ráta tulajdonságait tárgyalja, ehhez a részhez elsődleges forrásom Simonyi Gábor On Witsenhausen's zero-error rate for multiple sources [11] című 2001-es cikke volt.

2. Entrópia

Mielőtt rátérnénk dolgozatunk fő témájára, a zéró-hibájú információküldésre és gráfkapacitások fogalmára, először bemutatunk néhány alapfogalmat az általános információelméletből.

A témakör egyik legfontosabb fogalma az entrópia.

2.1. Definíció. Adott egy véges X halmazon egy P valószínűségi eloszlás. Ekkor P entrópiája

$$H(P) = \sum_{x \in X} -P(x) \log P(x)$$

A definícióhoz érdemes megjegyezni, hogy a témakörben log a 2-es alapú logaritmust jelenti, illetve úgy definiáljuk, hogy $0 \log 0 = 0$. Ez annyiban indokolt, hogy

$$\lim_{x \searrow 0} x \log x = 0.$$

Ennek a fogalomnak a bevezetését az alábbi kérdés motiválja:

Adott egy véges X betűhalmaz, amiből egymástól függetlenül P valószínűségi eloszlással érkeznek betűk a forrásból. Az adó az így kapott betűket szeretné minél hatékonyabban továbbítani a vevőnek egy bináris kóddal.

Az $f : X^k \to \{0,1\}^n$ és $\varphi : \{0,1\}^n \to X^k$ függvény-párt blokk-kódnak nevezzük, a függvények azt jelölik, hogy az adó f szerint küld bináris üzenetet, a vevő pedig azt φ szerint dekódolja.

Ekkor a hiba valószínűsége, tehát azé, hogy a vevő nem azt a betűsort dekódolja, ami a forrásból érkezett,

$$e(f, \varphi) = \Pr[\varphi(f(X^k)) \neq X^k]$$

2.2. Definíció. Adott k pozitív egészre és $\varepsilon > 0$-ra $n(k, \varepsilon)$-nal jelöljük a legkisebb olyan n-et, amire létezik $f : X^k \to \{0,1\}^n$ és $\varphi : \{0,1\}^n \to X^k$ blokk-kód, amire a hiba valószínűsége $e(f, \varphi) \leq \varepsilon$.

2.3. Tétel (Shannon forráskódolási tétele)**.** *Egy X véges halmazon megadott P valószínűségi eloszlás mellett*

$$\lim_{k \to \infty} \frac{n(k, \varepsilon)}{k} = H(P)$$

minden $\varepsilon > 0$-ra.

Ez tulajdonképpen azt jelenti, hogy elég hosszú blokkokat használva átlagosan $H(P)$ bit elküldése kell egy betűnyi információ továbbításához, kis valószínűségű hibát megengedve.

Ennek a tételnek egyszerű következménye az alábbi, hasznos állítás:

2.4. Állítás. *Egy X betűhalmazon értelmezett tetszőleges P valószínűségi eloszlásra*

$$H(P) \leq \log |X|$$

.

Bizonyítás. Ha $|X|^k$ minden elemének külön kódot adunk, az tetrmészetesen hiba nélkül dekódolható, és

$$n = \lceil \log |X|^k \rceil$$

bit kell hozzá, tehát az optimális átküldési arány,

$$H(P) \leq \lim_{k \to \infty} \frac{1}{k} \lceil \log |X|^k \rceil = \log |X|.$$

□

Ugyanez az állítás algebrailag is bizonyítható, az alábbi lemma segítségével:

2.5. Lemma.

$$\sum_{i=1}^{n} x_i \log x_i \geq \left(\sum_{i=1}^{n} x_i \right) \log \frac{\sum_{i=1}^{n} x_i}{n}$$

Bizonyítás. Az $x \log x$ függvény második deriváltja $\frac{1}{x} > 0$, tehát a függvény konvex, így használható rá a Jensen-egyenlőtlenség, a Lemmában szereplő egyenlőtlenség ezzel ekvivalens.

□

Ennek segítsgével pedig valóban kijön, hogy egy n elemű X halmazra

$$H(P) = -\sum_{x \in X} P(x) \log P(x) \leq -\left(\sum_{x \in X} P(x) \right) \log \frac{\sum_{x \in X} P(x)}{n} = -1 \cdot \log \frac{1}{n} = \log n = \log |X|$$

Érdemes még bevezetnünk a feltételes entrópia fogalmát:

2.6. Definíció.

$$H(Y|X) = \sum_{x \in X} P_X(x) H(Y|X = x)$$

A feltételes entrópiáról alapvető állítás az alábbi, ami akár alternatív definícióként is használható:

2.7. Tétel.

$$H(Y|X) = H(X,Y) - H(X)$$

Ebből következik az alábbi, "láncszabály"-nak nevezett felírás:

$$H(X_1,...,X_n) = H(X_1) + H(X_2|X_1) + H(X_3|X_1,X_2) + ... + H(X_n|X_1,...,X_{n-1})$$

Bizonyítás.

$$H(X,Y) = -\sum_{x\in X, y\in Y} P(x,y)\log P(x,y)$$
$$= -\sum_{x\in X}\sum_{y\in Y} P_X(x)P_Y(y|X=x)\log(P_X(x)P_Y(y|X=x))$$
$$= -\sum_{x\in X} P_X(x)\left(\sum_{y\in Y} P_Y(y|X=x)\log P_X(x) + \sum_{y\in Y} P_Y(y|X=x)\log P_Y(y|X=x)\right)$$
$$= -\sum_{x\in X} P_X(x)(\log P_X(x) - H(Y|X=x)) = H(X) + \sum_{x\in X} P_X(x)H(Y|X=x)$$

Tehát valóban

$$H(Y|X) = \sum_{x\in X} P_X(x)H(Y|X=x) = H(X,Y) - H(X)$$

□

Érdemes még megemlíteni az úgynevezett közös információ fogalmát:

Legyen W egy sztochasztikus mátrix, ami egy véges X betűhalmazból egy véges Y betűhalmazba képző csatornát reprezentál: ha egy $x \in X$ betűt küldenek át a csatornán, akkor $W(y|x)$ valószínűséggel jelenik meg y a csatorna túloldalán.

Ekkor egy X halmazon értelmezett P valószínűségi eloszlásra legyen

$$H(W|P) = \sum_{x\in X} P(x)H(W(\cdot|x),$$

ez azt mutatja, hogy ha P eloszlással sorsoljuk ki a csatornán átküldött betűt, akkor várható értékben $H(W|P)$ lesz a kimeneti betű eloszlásának entrópiája, ha már ismerjük a beküldött x betűt.

Mivel W egy sztocahisztikus mátrix, így WP maga is egy valószínűségi eloszlás Y-on, méghozzá a kimenet valószínűségi eloszlása, ha a bemenetet P szerint sorsoljuk ki.

2.8. Definíció. A P valószínűségi eloszlás mellett legyen $I(P,W)$ a bemenet ismeretéből kapott információ a kimenetre, ahol

$$I(P,W) = H(WP) - H(W|P)$$

Ez a mennyiség azt kívánja kifejezni, hogy várható értékben mennyivel csökken számunkra a kimenet bizonytalansága (entrópiája), ha megismerjük a bemenetet.

3. Kapacitás fogalmak

3.1. Csatornák ε-kapacitása

Most rátérünk az információelmélet egyik alapvető kérdéskörére, a zajos csatornák problémájára.

Az adó üzenetet szeretne küldeni a vevőnek, azonban a csatornán átküldött betűk nem pontosan érkeznek át, és van esélye, hogy két különböző elküldött betű ugyanúgy jelenik meg a csatorna túloldalán, így a dekódolás nem egyértelmű.

A W csatornát leírhatjuk mátrixként:

X az adó által küldhető bemeneti betűk halmaza, és Y a csatorna másik oldalán megjelenő kimeneti betűk halmaza, és $W(b|a)$-val jelöljük annak a valószínűségét, hogy ha a betű volt a bemenet, akkor b betű jelenik meg a csatorna túloldalán kimenetként.

Dolgozatunkban kizárólag az úgynevezett "emlékezet nélküli" csatornákkal foglalkozunk. Ezekre több betű elküldése esetén betűnként független esemény, hogy mi jelenik meg kimenetként. Üzenetküldésre n-betűs szavakat használunk. Egy $x \in X^n$ szót elküldve $W^n(y|x)$ valószínűséggel jelenik meg $y \in Y^n$ szó a túloldalon, ahol $x = x_1...x_n$ és $y = y_1...y_n$ szavakra

$$W^n(y|x) = \prod_{i=1}^{n} W(y_i|x_i).$$

Továbbá

3.1. Jelölés. $A \subset Y^n$ halmazra $W^n(A|x) = \sum_{y \in A} W^n(y|x)$.

Üzenetek egy M halmazát akarja az adó elkódolni a vevőnek, a kódot egy $f : M \to X^n$ kódoló, és egy $\varphi : Y^n \to M$ dekódoló függvény adja meg. Ha az adó az $m \in M$ üzenetet akarja kódolni, akkor elküldi a csatornán az $f(m) \in X^n$ kódot, a csatornán kijön egy $y \in Y^n$ kimeneti szó, és a vevő ezt $\varphi(y)$-ként dekódolja.

3.2. Jelölés. $\varphi^{-1}(m) = \{y \in Y^n : \varphi(y) = m\}$

f és φ akkor adnak ε-jó kódot,

$$W^n(\varphi^{-1}(m)|f(m)) \geq 1 - \varepsilon$$

minden $m \in M$ üzenetre, azaz bármilyen üzenetet kell is elküldeni, ε-nál kisebb az esélye, hogy a vevő azt rosszul dekódolja.

3.3. Definíció. Legyen $M(n)$ a legnagyobb olyan M üzenethalmaz mérete, aminek létezik ε-jó kódolása n-hosszú szavakkal.

Definiáljuk a gráf ε-kapacitását, ami azt fejezi ki, hogy optimiális kódokkal betűnként hány bit információ küldhető át a csatornán, formálisan

3.4. Definíció.

$$C_\varepsilon(W) = \sup_{n\in\mathbb{Z}^+} \frac{1}{n} \log M(n)$$

A csatorna kapacitása pedig ezeknek az értékeknek az infémuma,

$$C(W) = \lim_{\varepsilon\to 0} C_\varepsilon.$$

Erről egy fontos tétel az alábbi:

3.5. Tétel (Shannon csatornakódolási tétel)**.** *Minden* $0 < \varepsilon < 1$*-re*

$$C_\varepsilon = C = \max_P I(P, W)$$

Ennek a tételnek a bizonyítása megtalálható Csiszár és Körner Information Theory című könyvének 6. fejezetében, azonban itt kihagyom a bizonyítást, mivel jelen dolgozatom témaja inkább a zéró-hiba kommunikáció és az ehhez kapcsolódó, kombinatorikai jellegű problémák, így ez a tétel az ε-hibájú kommunikációról csak kontextust ad a következőkben szereplő tételekhez.

3.2. Gráfok Shannon-kapacitása

Minket jobban érdekel az az eset, amikor úgy kell az üzenetek kódját a csatornán átküldeni, hogy ε valószínűségű hibát sem engedünk meg, hanem a vevőnek minden esetben ki kell találnia, mi volt az eredeti üzenet.

Legyen egy n-hosszú x kódszóra és W csatornára

$$S_W(x) = \{y \in Y^n : W^n(y|x) > 0\}.$$

A hiba nélkül dekódolható információküldéshez az kell, hogy az adó egy olyan $C \subset X^n$ halmazból válassza az elküldött üzeneteket, amelyben semelyik két szó sem eredményezheti ugyanazt a kimenetet a csatorna túloldalán, azaz $S_W(x_1) \cap S_W(x_2) = \emptyset$ minden $x_1 \neq x_2 \in C$ kódszó-párra.

$N(W, n)$-nel jelöljük a legnagyobb $C \subset X^n$ kódszó-halmaz méretét, amelynek megvan ez a tulajdonsága.

3.6. Definíció. Egy W csatorna zéró-hiba kapacitása

$$C_0(W) = \sup_n \frac{1}{n} \log N(W, n).$$

Ez a definció azt fejezi ki, hogy optimális blokk-kódokat használva, bitenként mennyi információ küldhető át a csatornán.

Megmutatjuk, hogy ez a fogalom gráfok tulajdonságaként is kifejezhető:

Minden W csatornához tartozik egy $G(W)$ gráf, amelynek a csúcsai X elemei és x_1 és x_2 betűk akkor vannak összekötve, ha $S_W(x_1)$ és $S_W(x_2)$ halmazok diszjunktak, azaz ha a két betű összetéveszthetetlen.

Egy G gráf G^n hatványát a ko-normális gráf-szorzáson keresztül definiáljuk: G^n csúcshalamaza $V(G)^n$ és $(v_1, v_2, ..., v_n)$ és $(w_1, w_2, ..., w_n)$ csúcs-sorozatok pontosan akkor szomszédosak, ha létezik olyan $1 \leq i \leq n$, hogy v_i és w_i szomszédosak G-ben.

Ekkor észrevehetjük, hogy $G(W)^n = G(W^n)$, mivel $G(W^n)$ csúcsai az n-hosszú szavak, és két szó éppen akkor van összekötve, ha nem összetéveszthetőek, vagyis van olyan hely a két szóban, ahol olyan betűk állnak, amik nem adhatják ugyanazt a képet W-ben.

3.7. Jelölés. Egy G gráf klikkszámát $\omega(G)$-vel jelöljük, ez a G gráf maximális klikkjének csúcsszámát jelenti.

Észerevehetjük, hogy az n-hosszú kódszavak egy C részhalmaza pontosan akkor ad megfelelő kódot, ha az elemei klikket alkotnak a $G(W)^n$-ben, mivel az jelenti azt, hogy a kódszavak nem összetéveszthetőek.

Tehát értelmes definiálnunk az alábbi mennyiséget:

3.8. Definíció. [9]

A G gráf Shannon-kapacitása

$$C(G) = \sup_n \frac{1}{n} \log \omega(G^n).$$

Az imént megmutattuk, hogy ez ekvivalens a zéró-hiba információküldéshez tartozó kapacitással, azaz

3.9. Állítás.

$$C_0(W) = C(G(W))$$

3.10. Megjegyzés. Fontos megjegyezni, hogy Shannon eredetileg a gráf komplementerével vezette be a fogalmat, és a mai napig az irodalom jelentős részében ezt használják:

Az alternatív jelölés mellett egy W csatornához tartozó $G(W)$ gráfban éppen az összetéveszthető betűk vannak összekötve, és ebben az alternatív jelölésben C_{AND}-del jelöljük a Shannon-kapacitást, és

$$C_{AND}(G) = \sup_n \frac{1}{n} \log \alpha(G^n),$$

ahol α a gráf függetlenségi száma és a gráf-hatványozás is másképpen történik: két sorozat akkor van összekötve, ha minden helyen azonos vagy szomszédos betű szerepel bennük.

Ezen dolgozat nagy részében azonban a Csiszár-Körner könyvben használt, fentebb bemutatott definíciót használjuk, mivel látni fogjuk, hogy az irányított gráfokra vonatkozó Sperner-kapacitás esetén ez a definíció lényegesen természetesebb.

Dolgozatunk végén, a Witsenhausen-ráta tárgyalásánál majd részletesebben is foglalkozunk a C_{AND} alternatív jelöléssel.

Fontos észrevenni, hogy a Shannon-kapacitás definíciójában a szuprémum valójában a limit:

3.11. Tétel.

$$C(G) = \lim_{n\to\infty} \frac{1}{n} \log \omega(G^n)$$

Bizonyítás. Könnyű látni, hogy ha B egy klikk G^n-ben és C egy klikk G^m-ben, akkor $B \times C$ egy klikk G^{m+n}-ben, így $\omega(G^{m+n}) \geq \omega(G^m)\omega(G^n)$.

Legyen $a_n = \log \omega(G^n)$. Ekkor az előző szerint $a_{m+n} \geq a_m + a_n$, és minden a_n nemnegatív, ugyanis minden gráfban van egy-csúcsú klikk. Belátjuk, hogy ennyi feltétel elég ahhoz, hogy $\frac{a_n}{n}$ konvergál a szuprémumához.

□

3.12. Lemma (Fekete-lemma)**.** *Ha a nem-negatív a_n sorozat szuperadditív, azaz $a_{m+n} \geq a_m + a_n$ minden $m, n \in \mathbb{Z}^+$-ra, akkor $\frac{a_n}{n}$ konvergens és*

$$\lim_{n\to\infty} \frac{a_n}{n} = \sup_n \frac{a_n}{n}$$

Bizonyítás. Tetszőleges $n \geq 1$-re igaz, hogy minden m pozitív egész felírható $cn + d$ alakban, ahol $0 \leq d < n$, így

$$a_m \geq a_n + a_n + ... + a_n + a_d = ca_n + a_d \geq ca_n + \min\{0, a_1, ..., a_{n-1}\},$$

ahol ezt a csak n-től függő minimumot h_n-nel jelöljük. Ekkor

$$\frac{a_m}{m} \geq \frac{ca_n + h_n}{cn + d} \geq \frac{cn}{cn + d}(\frac{a_n}{n} + \frac{h_n}{cn})$$

Ahogy c tart a végtelenhez, úgy $\frac{h_n}{cn} \to 0$ és $\frac{cn}{cn+d} \to 1$, így

$$\liminf_{m\to\infty} \frac{a_m}{m} \geq \frac{a_n}{n}.$$

Ez minden $n \geq 1$-re teljesül, ezért

$$\liminf_{m\to\infty} \frac{a_m}{m} \geq \sup \frac{a_n}{n}.$$

Eközben nyilvánvalóan

$$\limsup_{m\to\infty} \frac{a_m}{m} \leq \sup \frac{a_n}{n},$$

így valóban létezik a határérték és

$$\lim_{n\to\infty} \frac{a_n}{n} = \sup \frac{a_n}{n}.$$

□

Sajnos általánosságban nehéz meghatározni egy gráf Shannon-kapacitását, csak néhány speciális gráfét ismerjük.

Sokáig a terület fontos nyitott kérdése volt az 5 csúcsú kör Shannon-kapacitása. Nem nehéz ellenőrizni, hogy ha G az 5 csúcsú kör, akkor G^2-ben található egy 5 csúcsú klikk, így

$$C(G) = \sup_n \frac{1}{n} \log \omega(G^n) \geq \frac{1}{2} \log \omega(G^2) = \frac{1}{2} \log 5.$$

Ennek a becslésnek az élességét végül Lovász László bizonyította egy új, a kapacitást felülről becsülő, θ-nak elnevezett gráfparaméterrel, amelynek viselkedését azóta is sokan kutatják.

3.13. Tétel (Lovász)**.** *[7]*

Az 5 *csúcsú kör Shannon-kapacitása* $\frac{1}{2} \log 5$.

Ennek a tételnek a bizonyítása sok helyen megtalálható magyar nyelven is, köztük Schwarcz Tamás 2018-as BSc szakdolgozatában [13], ezért úgy döntöttem, hogy nem mutatom be újra ezt a bizonyítást, helyette a többi kapacitás-fogalomra helyezek nagyobb hangsúlyt.

3.3. Csatornák családjának kapacitása informált vevővel

Fontos kérdéskör, hogy milyen hatékonyságú információátadás folytatható, ha az adó és vevő nem feltétlenül ismeri, hogyan működik a csatorna, amely összeköti őket.

Azt feltételezzük, hogy a csatorna mindenképp egy ismert X és Y betűhalmaz között vezet, illetve, hogy az adó és a vevő is ismerik azt a véges $\mathcal{W}$ halmazt, amiből a csatorna kikerülhet.

Először azt az esetet viszsgáljuk, amikor legalább a vevő tudja, hogy melyik csatorna van használatban.

Ha mindketten informáltak, az nem egy izgalmas probléma, ugyanis akkor egyszerűen minden lehetséges W csatornára készítenek külön egy arra a csatornára optimális kódot, és mikor mindketten látják, hogy a W csatorna kerül használatra, akkor az ahhoz tartozó kóddal kommunikálnak, tehát ennek a problémának a megoldásához nincsen szükségünk új fogalmakra.

Ha a vevő informált arról, hogy mi a csatorna, de az adó nem, az egy érdekesebb eset, most ezzel fogunk foglalkozni.

Ebben az esetben csatornák családjának is definiálhatjuk a kapacitását a fentiekkel analóg módon:

Legyen $N(\mathcal{W}, n)$ a legnagyobb M üzenethalmaz mérete, amire teljesül, hogy bármelyik csatorna is kerül használatra $\mathcal{W}$-ből, az adó tetszőleges üzenetet el tud küldeni M-ből, egy X^n-beli szót használva, úgy, hogy a megérkező Y^n-beli szóból a vevő egyértelműen dekódolni tudja, hogy mi volt az M-beli üzenet.

3.14. Definíció. A csatornák $\mathcal{W}$ családjának nulla-hibájú kapacitása

$$C_0(\mathcal{W}) = \sup_n \frac{1}{n} N(\mathcal{W}, n)$$

Minden $W \in \mathcal{W}$ csatornához vesszük a hozzá tartozó $G(W)$ gráfot, és $\mathcal{G}_{\mathcal{W}}$-vel jelöljük a

$$\{G(W) : W \in \mathcal{W}\}$$

családját a gráfoknak. Ekkor X^n-ben akkor jó kódszavak egy C halmaza, ha C elemei bármely $G \in \mathcal{G}_{\mathcal{W}}$ gráfra szomszédosak G^n-ben, azaz összetéveszthetetlenek a vevő számára.

Vagyis

$$C_0(\mathcal{W}, n) = \sup_n \frac{1}{n} \omega(\bigcap_{G \in \mathcal{G}_{\mathcal{W}}} G^n)$$

A 3.12 Tétellel megegyező módon belátható, hogy a szuprémum itt is egyben limesz,

$$C_0(\mathcal{W}) = \lim_{n \to \infty} \frac{1}{n} \omega(\bigcap_{G \in \mathcal{G}_{\mathcal{W}}} G^n).$$

Ennek a $C_0(\mathcal{W})$ értéknek a a meghatározása egy nehéz probléma, erre vontakozik majd a későbbiekben bemutatott Gargaon-Körner-Vaccaro-tétel.

Előtte azonban megvizsgálunk egy másik esetet is, hogy a bevezetett új fogalmakkal teljes általánosságában mondhassuk ki a Gargano-Körner-Vaccaro-tételt.

3.4. Csatornák családjának kapacitása nem informált vevővel

Most elkezdjük vizsgálni azt az esetet, amikor sem az adó, sem a vevő nem ismeri, hogy $\mathcal{W}$-ből melyik csatorna van használatban.

Először röviden megvizsgáljuk azt az esetet, amikor az adó informált arról, hogy $\mathcal{W}$ melyik csatornáját használják, csak a vevő nem.

Legyen $\mathcal{W} = \{W_1, W_2, ..., W_k\}$. Ha létezik olyan $W \in \mathcal{W}$, amiben bármely két X-beli betű adhatja ugyanazt a kimenetet a W csatornán, akkor semmilyen információ nem küldhető át hiba nélkül, mert ha éppen a W csatornát kell használnunk, akkor bármely két elküldött üzenet adhatja ugyanazt a kimeneti szót.

Ellenben, ha minden $W_i \in \mathcal{W}$-re léteznek x_i és z_i betűk, amik nem adhatják ugyanazt a kimenetet, akkor az $x_1 x_2 ... x_k$ és $z_1 z_2 ... z_k$ szavak nem összetéveszthetők semelyik $W_i \in \mathcal{W}$-re, így egy bitnyi információt már át tud küldeni az adó a vevőnek.

Ezt ismételve az adó korlátos sok lépésben meg tudja küldeni a vevőnek azt az információját, hogy melyik csatorna van használatban.

Ezzel korlátos sok lépésben visszavezethetik a problémát arra a helyzetre, amikor az adó és a vevő is informált, és a korlátos sok kezdeti lépés nem befolyásolja a limeszként megkapott kapacitást.

Mostantól azt az érdekesebb esetet vizsgáljuk, amikor sem az adó, sem a vavő nem iformált arról, hogy melyik csatorna van használatban.

Ehhez bevezetjük az alábbi hozzárendelést:

3.15. Definíció. $\mathcal{W}$ átmeneti sztochasztikus mátrixok egy családja egy közös X bemeneti és Y kimeneti ábécével. A mátrixok minden (V, W) rendezett párjához hozzárendeljük a $G_{(V,W)}$ irányított gráfot az X csúcshalmazon. Ebben a gráfban egy a betűből pontosan akkor fut él b-be, ha

$$S_V(a) \cap S_W(b) = \emptyset,$$

azaz ha az a betűt küldve a V csatornán és a b betűt küldve a W csatornán nem kaphatjuk ugyanazt a kimenetet.

Az így kapott irányított gráfok családját $\mathcal{G}(\mathcal{W})$-nek nevezzük, ez a $\mathcal{W}$-hez rendelt irányított gráfcsalád.

Most definiáljuk a kapacitást nem informált adóra és vevőre:

3.16. Definíció. A kódszavak egy $C \subset X^n$ halmaza megfelelő, ha létezik olyan $\varphi : Y^n \to C$ dekódoló függvény, hogy bármely $W \in \mathcal{W}$ csatorna és $x \in C$ kódszó esetén

$$W^n(\varphi^{-1}(x)|x) = 1,$$

azaz biztosan olyan kimenet érkezik a csatorna túloldalán, amit a vevő x-nek dekódol.

A legnagyobb ilyen megfelelő $C \subset X^n$ kódszó-halmaz méretét $N^*(\mathcal{W}, n)$-nel jelöljük.

A $\mathcal{W}$ család kapacitása nem informált vevővel ekkor

$$C_0^*(\mathcal{W}) = \sup_n \frac{1}{n} \log N^*(\mathcal{W}, n) = \lim_{n\to\infty} \frac{1}{n} \log N^*(\mathcal{W}, n)$$

$C \subset X^n$ akkor megfelelő kódzó-halmaz, ha tetszőleges C-beli (x, z) rendezett párra, ahol $x \neq z$ és $\mathcal{W}$-beli (V, W) (nem feltétlenül különböző) rendezett párra

$$S_V(x) \cap S_W(z) = \emptyset,$$

máskülönben a vevő nem tudna biztosan jó φ függvényt létrehozni, ugyanis kaphatna olyan kimenetet, amiről nem tudhatja, hogy az x bemenetből kapta a V mátrix szerint, vagy a z bemenetből a W mátrix szerint. Ha viszont ez a feltétel teljesül, akkor könnyű megfelelő φ dekódolást csinálni, mert minden kimeneti szó legfeljebb egy C-beli szóból származhat.

$$S_V(x) \cap S_W(z) = \emptyset$$

azzal ekvivalens, hogy van olyan i koordináta, amire

$$S_V(x_i) \cap S_W(z_i) = \emptyset,$$

azaz létezik olyan i koordináta, amire a $G_{(V,W)}$ gráfban x_i-ből él fut z_i-be. A gráfszorzás szabálya szerint ez azzal ekvivalens, hogy $G^n_{(V,W)}$-ben él fut x-ből z-be.

(A gráfszorzás irányított gráfokra az irányítatlan gráfszorzás természetes kiterjesztése, a formális definícióját hamarosan kimondjuk.)

Ennek minden rendezett (V, W) párra és rendezett $x \neq z \in C$ párra teljesülnie kell, tehát C bármely két pontja között mindkét irányba él fut minden $G^n_{(V,W)}$ gráfban.

Ezzel eljött az ideje, hogy bevezessük a gráfkapacitás fogalmát irányított gráfokra:

3.5. Sperner-kapacitás

3.17. Definíció. F és G irányított gráfok szorzata $F \cdot G$ csúcshalmaza a csúcshalmazok direkt-szorzata, és (v_1, w_1)-ből akkor vezet él (v_2, w_2)-be, ha v_1-ből él vezet v_2-be vagy w_1-ből éle vezet w_2-be. Egy gráf hatványa ezen a szorzáson keresztül definiált, azaz a hatvány-gráfban akkor vezet él az egyik csúcsból a másikba, ha legalább az egyik koordinátában él vezet.

3.18. Definíció. Egy G irányított gráfban S egy szimmetrikus klikk, ha S bármely két csúcsa között mindkét irányban él fut.

$\omega_S(G)$ jelzi a G irányított gráfban a legnagyobb szimmetrikus klikk méretét.

3.19. Definíció.

$$C(G) = \lim_{n\to\infty} \frac{1}{n} \log \omega_S(G^n)$$

az irányított gráf Sperner-kapacitása.

A Shannon-kapacitáshoz hasonlóan a Sperner-kapacitás is kiterjeszthető gráf-családokra:

3.20. Definíció. Irányított gráfok egy $\mathcal{G}$ családjának Sperner-kapacitása

$$C(\mathcal{G}) = \lim_{n\to\infty} \frac{1}{n} \log \omega_S(\bigcap_{G\in\mathcal{G}} G^n)$$

Mint látni fogjuk, a Shannon-kapactiás a Sperner-akapcitás egy speciális esete, ez indokolja a megegyező $C(G)$ jelölés használatát.

A limesz létezése ugyanúgy bizonyítható, mint a nem irányított gráf esetén, a 3.12 Farkas-lemma segítségével.

Mint az előző rész végén levezettük, nem infromált adó és vevő esetén $C \subset X^n$ pontosan akkor megfelelő kódszó-halmaz, ha C szimmetrikus klikk $\mathcal{G}(\mathcal{W})$ minden eleme szerint, azaz

$$C_0^*(\mathcal{W}) = C(\mathcal{G}(\mathcal{W})).$$

Érdemes megjegyezni, hogy az irányított gráfok és a Sperner-kapacitás vizsgálata teszi célszerűvé, hogy Csiszár és Körner, és őket követve ez a dolgozat is, azt a jelölést használja, hogy egy W csatornához rendelt $G(W)$ gráfban az összetéveszthetetlen betűk vannak összekötve.

A szakirodalom jelentős része ennek a definíciónak éppen a komplementerét használja. Az esetek többségében a két definíció hasonló kényelemmel használható, azonban a nem informált adó és vevő esetén irányított gráfok bevezetése szükséges, és itt az általunk használt jelölések lényegesen kényelmesebbek.

Érdemes még a név eredetét megemlíteni:

Ha G-nek 2 csúcsa van (nevezzük $\{0,1\}$-nek), amik között mindkét irányba él fut, akkor a G^n-beli $0-1$ vektorok tekinthetők egy n elemű halmaz részhalmazainak karakterisztikus vektoraként. Két vektor között akkor fut mindkét irányba él G^n-ben, ha létezik olyan koordináta, ahol az egyik 0 és a másik 1, és olyan is, ahol az egyik 1 és a másik 0, azaz mindkét vektorhoz tartozó halmaznak van olyan eleme, ami nincs benne a másik halmazban, vagyis egyik halmaz sem tartalmazza a másikat.

Tehát ekkor G^n-ben a legnagyobb szimmetrikus klikk keresése ekvivalens azzal a kérdéssel, hogy hány részhalmaza választható egy n elemű halmaznak úgy, hogy semelyik se tartalmazza a másikat. A Sperner-tétel azt mondja ki, hogy az ilyen részhalmazok maximális száma $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Fontos látni, hogy minden egyszerű gráf megkapható irányított gráfként, ahol két csúcs között vagy nem fut, vagy mindkét irányba fut él. Ilyenmódon a Shannon-kapacitás meghatározása egy speciális alesete a Sperner-kapacitás meghatározásának az ilyen fajtájú gráfokra. Éppen ezért a továbbiakban csak a Sperner-kapacitásról látunk be állításokat, mert ugyanazok érvényesek lesznek a Shannon-kapacitásra is.

Viszont általánosságban a gráfok irányítottsága nem elhagyható a Sperner-kapacitás definíciójából, ugyanannak az egyszerű gráfnak különböző irányításai más kapacitásúak lehetnek, amint ezt az alábbi szép tétel szemlélteti:

3.21. Tétel (Calderbank, Frankl, Graham, Li, Shepp). *[10]*

A három hosszú irányított kör Sperner-kapacitása $\log 2$*, míg a* 3 *csúcsú tranzitív tournament Sperner-kapacitása* $\log 3$*.*

Bizonyítás. Először a 3 csúcsú tranzitív G gráfra látjuk be az állítást. A csúcsokat $0, 1$ és 2 sorszámokkal látjuk el, két csúcs közül mindig a kisebb sorszámúból vezet él a nagyobb sorszámúba.

Vesszük az olyan $\{0,1,2\}^n$-beli vektorokat, amikben a koordináták összege n. Két különböző ilyen vektor között mindig mindkét irányban él fut a G^n gráfban, ugyanis a vektorok különbözősége miatt van olyan koordináata, ahol az egyik nagyobb mint a másik, és mivel az összeg megegyezik, lennie kell egy másik koordinátának, ahol pedig a másik nagyobb mint az egyik.

A centrális határeloszlás tételét használva az n összegű vektorok száma nagyságrendileg

$$\frac{3^n}{\sqrt{\frac{2}{3}n}\sqrt{2\pi}}$$

tehát

$$C(G) = \lim_{n\to\infty} \frac{1}{n} \log \omega_S(G^n) \geq \log 3$$

és világosan $C(G) \leq \log 3$, így az egyenlőség teljesül.

A 3 hosszú irányított kör esete ennél nehezebb, ehhez egy segédtételt fogunk belátni, amelyből kijön az állítás egy érdekes általánosítása.

□

3.22. Definíció. Vesszük egy G gráf összes szabályos c színezését. G minden v csúcsára megnézzük, hogy v szomszédai (vagy irányított gráf esetén kiszomszédai), v-t is beleértve hány színnel színezettek a c színezésben. Vesszük ezen értékek maximumát G csúcsai között, ez egy c színezésre jellemző érték. Az összes lehetséges c közül vesszük ennek az értéknek a minimumát, ez a lokális kromatikus szám, jele $\psi(G)$. Röviden,

$$\psi(G) = \min_c \max_{v\in V(G)} |c(\hat{N}(v))|$$

3.23. Tétel (Körner, Pilotto, Simonyi)**.** [12]
Ha G egy irányított gráf és $\overleftarrow{G}$-vel jelöljük azt az irányított gráfot, amit úgy kapunk, hogy G minden élének irányát megfordítjuk, akkor

$$C(G) \leq \min\{\log \psi(G), \log \psi(\overleftarrow{G})\}$$

Bizonyítás. A polinomiális módszer segítségével bizonyítjuk az állítást. G egy c színezésében minden színhez hozzárendelünk egy különböző valós számot.

Legyen A olyan n hosszú vektorok halmaza, amik szimmetrikus klikket alkotnak G^n-ben. Minden $a = (a_1, ..., a_n) \in A$ vektorhoz hozzárendeljük az alábbi polinomot:

$$f_a(x_1, x_2, ..., x_n) = \prod_{i=1}^{n} \prod_{b\in c(N_+(a_i))} (x_i - b),$$

ahol a második produktum az a_i csúcs kiszomszédjain fut végig.

$f_a(x_1, x_2, ..., x_n)$ pontosan akkor 0, ha valamelyik x_i érték a_i egy kiszomszédja színének felel meg.

Ha az A-beli csúcs-sorozatokhoz tartozó színsororozatokat helyettesítjük be f_a-ba, akkor az a-hoz tartozó színsorozatra 0-tól különböző értéket kapunk, mivel a színezésben nem kerülhetnek azonos színek szomszédos csúcsokra, viszont minden a-tól különböző A-beli csúcs-sorozatra $f_a = 0$, mivel A elemei szimmetrikus klikket alkotnak G^n-ben.

Tehát az $a \in A$ vektorokhoz rendelt f_a polinomok mind függetlenek, mert egy lineáris kombinációjuk csak akkor vehet föl 0 értéket az összes A-hoz tartozó színezésen, ha mindegyik polinom súlya 0.

Másrészt mindegyik polinomnak n változója van, és minden változó legfeljebb

$$\max_{v \in V(G)} |c(N(v))|$$

kitevővel szerepel, így a lehetséges monomok száma legfeljebb

$$\left(1 + \max_{v \in V(G)} |c(N(v))|\right)^n,$$

tehát a polinomok tere legfeljebb ennyi dimenziós, vagyis

$$|A| \leq \left(\max_{v \in V(G)} |c(\hat{N}(v))|\right)^n$$

Ez minden c színezésre teljesül, ezért

$$|A| \leq \psi(G)^n.$$

Mivel ez minden A szimmetrikus klikkre igaz, ezért $C(G)$ definíciójából következően

$$C(G) \leq \log \psi(G).$$

Mivel vektorok egy halmaza pontosan akkor szimmetrikus klikk G^n-ben, mint $\overleftarrow{G}^n$-ben, ezért ugyanazen bizonyítással belátható, hogy

$$C(G) \leq \log \psi(\overleftarrow{G}),$$

ezzel a tételt beláttuk.

□

Most már rátérhetünk a 3-hosszú kör kapacitására, egy általánosabb állítást bizonyítva:

3.24. Tétel (Körner, Pilotto, Simonyi)**.** *[12]*

Egy páratlan kör szinte minden irányításának $\log 2$ *a Sperner-kapacitása. Az egyetlen lehetséges kivétel a kvázi-alternáló irányítás, amiben egy kivételével minden csúcs kifoka* 0 *vagy* 2*.*

3.25. Megjegyzés. Érdemes megjegyezni, hogy ennek a tételnek a bizonyítása sok, egymásra épülő tételen keresztül történt, először A.R. Calderbank, P. Frankl, R.L. Graham, W.-C.W. Li és L.A. Shepp bizonyították az állítást háromszögre [10], később Blokhuis [2] újra bizonyította az itt bemutatott polinomiális módszerrel, majd ezt a bizonyítást Noga Alon [1] általánosította, és végül erre építve mondta ki Körner, Pilotto és Simonyi az itt szereplő tételt.

Bizonyítás. Egy n csúcsú körben a kifokok összege n, ez páratlan, tehát páratlan sok csúcsnak 1 a kifoka, vagyis egy nem kvázi-alternáló irányításban legalább három olyan csúcs van, aminek 1 a kifoka.

Kiválasztunk három ilyen csúcsot. Ha bármely kettő között páratlan a távolság, akkor beszínezzük őket három különböző színre, és két kiválasztott csúcs közti köríven felváltva színezzük a csúcsokat a két végpont színével. Ekkor mindegyik csúcsnak csak egyféle színű kiszomszédja van.

Ha a kiválasztott csúcsok közül A és B csúcsok távolsága páratlan és B és C, illetve C és A távolsága páros, akkor C-ből pontosan az egyik irányba mutat kifele él, az általánosság rovása nélkül feltehető, hogy B irányába. Ekkor B-t kékre, A-t és C-t pedig pirosra színezzük. Az AB körív és a CA körív csúcsait felváltva színezzük kékre és pirosra, ez a paritások miatt helyesen megtehető. A BC körív csúcsait pedig kékre és sárgára színezzük felváltva B-től kezdve, amíg bele nem ütközünk a piros színű C csúcsba. Ekkor is teljesül, hogy mindegyik csúcsnak csak egyféle színű kiszomszédja van.

Tehát $\psi(G) = 2$. Ebből következik az előző tétel alapján, hogy $C(G) \leq \log 2$.

Másrészt $\log 2$ kapacitás már egy egyetlen irányított élből álló gráffal is elérhető:

A két csúcsot 0-nak és 1-nek nevezzük, és vesszük azokat a vektorokat, amikben az összeg $\lfloor \frac{n}{2} \rfloor$. Bármely két ilyen vektor esetén van olyan koordináta ahol az egyik, és olyan, ahol a másik nagyobb, és ezen vektorok száma $\binom{n}{\lfloor \frac{n}{2} \rfloor}$, és

$$\lim_{n\to\infty} \frac{1}{n} \log \binom{n}{\lfloor \frac{n}{2} \rfloor} = \log 2,$$

tehát $C(G) = \log 2 = 1$.

□

4. Gargano-Körner-Vaccaro-tétel

4.1. Kapacitás típusokon belül

Meilőtt kimondhatnánk a gráf-családokra vonatkozó központi tételünket, a Gargano-Körner-Vaccaro-tételt, még be kell vezetnünk egy, az információelméletben több helyen hasznos fogalmat.

4.1. Definíció. $T_P \subset X^n$ a P típusú szavak halmaza, azaz azon n-hosszú szavak halmaza, amiben X betűinek eloszlása éppen P.

Az n-hosszú szavak között előforduló betűeloszlások halmazát $\mathcal{P}_n$-nel jelöljük, $|\mathcal{P}_n|$ a különböző típusok száma, és erre egy felső becslést ad az alábbi, rendkívül egyszerű, de meglepően fontos lemma:

4.2. Lemma (Típus számláló lemma)**.** [5]
$|\mathcal{P}_n| \leq (n+1)^{|X|}$

Bizonyítás. Mind az $|X|$ különböző betű száma 0 és n között van a szóban, így a lehetséges eloszlások száma legfeljebb $(n+1)^{|X|}$.

$\square$

Az egy típusba tartozó szavak számáról is kimondunk egy hazsnos lemmát:

4.3. Lemma. *A véges X halmazon veszünk $P_1, P_2, \ldots$ eloszlásokat, ahol $P_n \in \mathcal{P}_n$ és a $P_1, P_2, \ldots$ eloszlások a P eloszláshoz konvergálnak abban az értelemben, hogy*

$$\sup_{x\in X} |P_n(x) - P(x)| \to 0,$$

ahogy n tart a végtelenhez. Ekkor teljesül, hogy

$$\lim_{n\to\infty} \frac{1}{n} \log |T_{P_n}| = H(P)$$

Bizonyítás.

$$|T_{P_n}| = n! \prod_{x\in X} \frac{1}{(nP_n(x))!},$$

így a Stirling-formula szerint

$$\lim_{n\to\infty} \frac{1}{n} \log |T_{P_n}| = \lim_{n\to\infty} ((\log n - 1) - \sum_{x\in X} P_n(x)(\log n + \log P_n(x) - 1)) = -\sum_{x\in X} P(x) \log P(x) = H(P)$$

$\square$

A típusokat gyakran érdemes kissé tágabban értelmezni:

4.4. Definíció. Legyen $[P]_\delta$ azon Q eloszlások halmaza, amikre $|P(x) - Q(x)| \le \delta$ minden $x \in X$-re, és legyen $T_{[P]_\delta} \subset X^n$ azon sorozatok halmaza, amiknek a típusa $[P]_\delta$-ba tartozik.

Ezek segítségével már definiálhatjuk a következő segédfogalmat:

4.5. Definíció. Legyen $G^n[P,\delta]$ a G^n gráf feszített részgráfja a $T_{[P]_\delta}$-hoz tartozó csúcsokon.

Ekkor legyen

$$C(G,P) = \lim_{\delta\to 0} \limsup_{n\to\infty} \frac{1}{n} \log \omega(G^n[P,\delta]),$$

és egy csatorna nulla-hibájú kapacitása egy adott P eloszlás mellett

$$C_0(W,P) = C(G(W),P).$$

A későbbiekben többször is használni fogjuk az alábbi lemmát:

4.6. Lemma. *Legyenek a véges V halmazon $P_n \in \mathcal{P}_n$ valószínűségi eloszlások, amik P-hez konvergálnak abban az értelemben, hogy*

$$\sup_{x\in X} |P_n(x) - P(x)| \to 0,$$

ahogy n tart a végtelenhez. Ekkor ha adott G gráf a V halmazon, akkor

$$C(G, P) = \lim_{n\to\infty} \frac{1}{n} \log \omega(G^n[P_n, 0])$$

Bizonyítás. Először belátjuk, hogy tetszőleges $\delta > 0$ mellett

$$\limsup_{n\to\infty} \frac{1}{n} \log \omega(G^n[P, \delta]) = \lim_{n\to\infty} \frac{1}{n} \log \omega(G^n[P, \delta]).$$

Ennek bizonyítása megegezik a 3.12 tételével, ugyanis itt is teljesül, hogy egy $G^m[P, \delta]$ és egy $G^n[P, \delta]$-beli klikk direkt-szorzata klikk G^{m+n}-ben, és egy $G^n[P, \delta]$-beli és egy $G^m[P, \delta]$-beli sorozat összefűzésében minden betű előfordulási aránya az arányok konvex kominációja lesz, így az összfűzéssel kapott sorozat is $G^{m+n}[P, \delta]$-ban van.

Tehát mostantól használhatjuk azt a definíciót, hogy

$$C(G, P) = \lim_{\delta\to 0} \lim_{n\to\infty} \frac{1}{n} \log \omega(G^n[P, \delta]).$$

Tetszőleges $\delta > 0$-ra létezik olyan N, hogy $\forall n > N$-re

$$P_n \in [P]_\delta,$$

így $C(G, P)$ definíciójából következően

$$C(G, P) \geq \limsup_{n\to\infty} \frac{1}{n} \log \omega(G^n[P_n, 0])$$

Másrészt $C(G, P)$ definíciója szerint minden $\delta > 0$-ra és $\varepsilon > 0$-ra teljesül, hogy kellően nagy n-re

$$\frac{1}{n} \log \omega(G^n[P, \delta]) \geq C(G, P) - \varepsilon.$$

Legyen továbbá n elég nagy ahhoz, hogy $P_n \in [P]_\delta$ is teljesüljön.

$T_{[P]_\delta} \subset X^n$ felbontható Q_i típusú halmazok diszjunkt uniójára, ahol minden Q_i-re igaz, hogy minden $x \in X$-re a Q_i típusú vektorokban az x betűk száma legfeljebb $n(P(x) + \delta)$.

Tegyük föl először, hogy $P(x) \neq 0$ semely $x \in X$-re. Legyen

$$\min_{x\in X} P(x) = s,$$

és legyen

$$(1 + \frac{4\delta}{s})n < k < (1 + \frac{5\delta}{s})n,$$

és vegyünk egy $P' \subset [P]_\delta$ eloszlást $\mathcal{P}_k$-ban, amire $P'(x) > 0$ minden $x \in X$-re.

Ekkor minden $T_{Q_i} \subset T_{[P]_\delta}$-ra és minden $x \in X$ betűre, a P' típusú k hosszú sorozatokban több x betű szerepel, mint a Q_i típusú n hosszú sorozatokban.

Ekkor a $G^n[P, \delta]$-ban klikket alkotó sorozatok mindegyikének a végére odafűzhetünk egy $k - n$ hosszú végződést, amivel együtt mindegyiknek P' lesz a típusa. Az így kapott sorozatok klikket alkotnak $G^t[P', 0]$-ban. Ezek szerint

$$\omega(G^n[P, \delta]) \leq \omega(G^k[P', 0]).$$

Tehát ha egy

$$(1 + \frac{4\delta}{s})n < k < (1 + \frac{5\delta}{s})n$$

esetén igaz P_k-ra, hogy minden $x \in X$-hez pozitív súlyt rendel, akkor

$$C(G, P) - \varepsilon \leq \frac{1}{n} \log \omega(G^n[P, \delta]) \leq (1 + \frac{5\delta}{s})\frac{1}{k} \log \omega(G^k[P_k, 0]).$$

Ha a P eloszlás minden $x \in X$-hez pozitív súlyt rendel, akkor létezik K, hogy $k > K$-ra $P_k(x)$ is pozitív minden $x \in X$-re, tehát teljesül rá az előbbi állítás.

Ekkor tetszőleges $\varepsilon > 0$ és $\delta > 0$-ra igaz, hogy kellően nagy k-ra

$$\frac{C(G, P) - \varepsilon}{1 + \frac{5\delta}{s}} \leq \frac{1}{k} \log \omega(G^k[P_t, 0]),$$

vagyis ekkor valóban teljesül, hogy

$$C(G, P) \leq \liminf_{n \to \infty} \frac{1}{n} \log \omega(G^n[P_n, 0]).$$

Meg kell még vizsgálni azt az esetet, amikor létezik $x \in X$, amire $P(x) = 0$. Itt indukcióval bizonyítjuk az olyan $x \in X$ betűk száma szerint, amikre $P(x) = 0$, azt az állítást, hogy

$$C(G, P) \leq \liminf_{n \to \infty} \frac{1}{n} \log \omega(G^n[P_n, 0]).$$

Az az indukció alapesete, ha egyetlen olyan betű sincs, amire $P(x) = 0$, és azt bizonyítottuk az imént.

Ha egy adott $x \in X$-re $P(x) = 0$, akkor $T_{[P]_\delta}$ minden sorozatában legfeljebb $n\delta$ darab x betű van, így az x betűk lehetséges elhelyezkedéseinek száma az n hosszú sorozatban

$$\binom{n}{0} + \binom{n}{1} + ... + \binom{n}{n\delta} \leq n\delta n^{n\delta} \leq n^{1+n\delta}$$

tehát létezik egy legalább

$$\frac{\omega(G^n[P,\delta])}{n^{1+n\delta}}$$

mérteű klikk $G^n[P,\delta]$-ban olyan sorozatokból, amikben az x betűk ugynott vannak, ezekből az összes, t darab, x betűt elhagyva egy $G^{n-t}[\overline{P},2\delta]$-beli klikket kapunk, ahol $\overline{P}$ értelemzési tartományában nem szerepel az x betű, a többi betűre pedig $\overline{P}(Y) = P(y)$.

Tehát

$$\omega(G^n[P,\delta]) \leq n^{1+n\delta}\omega(G^{n-t}[\overline{P},2\delta])$$

Mivel

$$\frac{1}{n}\log n^{1+n\delta} \to \delta,$$

és $\frac{n-t}{n} \geq 1-\delta$, és $C(G,P)$ definíciójában δ-val tartunk a 0-hoz, ebből az következik, hogy

$$C(G,P) = C(G,\overline{P})$$

Továbbá a P_n eloszlásokból is képezhetünk $\overline{P_n}$ eloszlásokat úgy, hogy az x betűket elhagyjuk. Mivel az x betűk számának (t_n) aránya tart a 0-hoz, ezért $\frac{n-t_n}{n}$ tart az 1-hez, így

$$\liminf_{n\to\infty}\frac{1}{n}\log\omega(G^n[P_n,0]) \geq \liminf_{n\to\infty}\frac{1}{n-t_n}\log\omega(G^{n-t_n}[\overline{P_n},0])$$

Mivel $\overline{P}$ eggyel kevesebb betűhöz rendel 0 súlyt, mint P, így erre alkalmazható az indukciós állítás, vagyis

$$C(G,\overline{P}) \leq \liminf_{n\to\infty}\frac{1}{n-t_n}\omega(G^{n-t_n}[\overline{P_n},0]),$$

vagyis

$$C(G,P) \leq \liminf_{n\to\infty}\frac{1}{n}\log\omega(G^n[P_n,0]).$$

Ezek szerint

$$\limsup_{n\to\infty}\frac{1}{n}\log\omega(G^n[P_n,0]) \leq C(G,P) \leq \liminf_{n\to\infty}\frac{1}{n}\log\omega(G^n[P_n,0]),$$

tehát valóban teljesül, hogy

$$\lim_{n\to\infty}\frac{1}{n}\log\omega(G^n[P_n,0]) = C(G,P).$$

□

Fontos még kimondanunk az alábbi tételt, amely segít rámutatni, hogy miért lesz hasznos a típusokon belül vett kapactiás fogalma:

4.7. Tétel.

$$C(G) = \max_P C(G, P)$$

Bizonyítás. Definíció szerint

$$C(G) = \lim_{n\to\infty} \frac{1}{n} \log \omega(G^n)$$

és

$$C(G, P) = \lim_{\delta\to 0} \lim_{n\to\infty} \omega(G^n[P, \delta]),$$

ebből világos, hogy

$$C(G) \geq \max_P C(G, P).$$

Legyen $\omega'(G^n)$ a legnagyobb olyan klikk mérete az n hosszú vektorok között, ahol minden vektor ugyanabba a típusba tartozik.

A 4.2 Típus számláló lemma szerint legfeljebb $(n+1)^{|X|}$ különböző típus van, ebből következően

$$\omega'(G^n) \geq \frac{1}{(n+1)^{|X|}} \omega(G^n),$$

ami azt jelenti, hogy

$$\lim_{n\to\infty} \frac{1}{n} \log \omega'(G^n) = \lim_{n\to\infty} \frac{1}{n} \log \omega(G^n) = C(G)$$

Egy adott n-re a maximális, $N'(\mathcal{G}, n)$ méretű, azonos típusba tartozó klikk típusát elnevezzük P_n-nek.

Az $|X|$-en értelmezett valószínűségi eloszlások tere kompakt a maximum-eltérés metrikában, így a $P_1, P_2, ...$ sorozatnak van egy konvergens részsorozata, ami egy P eloszláshoz konvergál.

Ekkor erre a P-re

$$C(G, P) = \lim_{\delta\to 0} \lim_{n\to\infty} \frac{1}{n} \log \omega(G^n[P, \delta]) \geq \lim_{n\to\infty} \frac{1}{n} \log \omega'(G, n) = C(G).$$

Ebből együtt tehát valóban következik, hogy

$$C(G) = \max_P C(G, P).$$

$\square$

4.2. A Gargano-Körner-Vaccaro-tétel kimondása

4.8. Tétel (Gargano-Körner-Vaccaro). *[14]*

Ha $\mathcal{G}$ irányított gráfok egy véges családja egy közös V csúcshalmazon, és P egy valószínűségi eloszlás V-n, akkor

$$C(\mathcal{G}, P) = \min_{G \in \mathcal{G}} C(G, P).$$

Ebből következően

$$C(\mathcal{G}) = \max_{P} \min_{G \in \mathcal{G}} C(G, P).$$

Ebből pedig következik, hogy egy $\mathcal{W}$ csatorna-családra iformált vevő mellett

$$C_0(\mathcal{W}) = \max_{P} \min_{W \in \mathcal{W}} C_0(W, P),$$

nem informált vevő mellett pedig

$$C_0^*(\mathcal{W}) = \max_{P} \min_{V \in \mathcal{W}, W \in \mathcal{W}} C(G_{(V,W)}, P).$$

A gráfokra vonatkozó 4.7 tétellel megegyező módon bizonyítható gráf-családokra is, hogy

$$C(\mathcal{G}) = \max_{P} C(\mathcal{G}, P),$$

ebből magától értetődően adódik a tételben szereplő első következtetés.

A csatorna-családokra vonatkozó következmények pedig világosan következnek abból, hogy az előző részekben már beláttuk, hogy a csatorna-családok kapacitása megegyezik a megfelelő gráfcsaládok Sperner-kapacitásával.

(Informált vevő esetén a gráfcsalád Shannon-kapacitását kellett vizsgálnunk, de ha az egyszerű gráfra úgy tekintünk, hogy minden éle helyén kétirányú él van, akkor a Shannon-kapacitás megegyezik a Sperner-kapacitással.)

Tehát már csak azt kell belátni, hogy

$$C(\mathcal{G}, P) = \min_{G \in \mathcal{G}} C(G, P).$$

Itt az egyik irányú egyenlőtlenség világos:

$$C(\mathcal{G}, P) \leq \min_{G \in \mathcal{G}} C(G, P),$$

mivel minden n-re magától értetődően teljesül, hogy

$$\omega(\bigcap_{G \in \mathcal{G}} G^n) \leq \min_{G \in \mathcal{G}} \omega(G^n, P).$$

Az egyenlőtlenség másik irányát az alábbi, központinak nevezett tételen keresztül mutatjuk meg:

4.9. Tétel (Központi tétel)**.** *[14]*

Ha $\mathcal{F}$ és $\mathcal{G}$ gráfcsaládok ugyanazon a V csúcshalmazon, és adott egy P valószínűségi eloszlás V-n, akkor

$$C(\mathcal{G} \cup \mathcal{F}, P) \geq \min\{C(\mathcal{F}, P), C(\mathcal{G}, P)\}.$$

Ha ezt már beláttuk, abból valóban következik a Gargano-Körner-Vaccaro-tétel:

A központi tételt használva az $\mathcal{F}_i = \{G_1, ..., G_{i-1}\}$ és $\mathcal{G}_i = \{G_i\}$ családokra induktívan megkapjuk, hogy

$$C(\mathcal{G}, P) \geq \min_{G \in \mathcal{G}} C(G, P).$$

4.3. Lemmák a központi tételhez

A központi tétel bizonyítása újabb fogalmak bevezetését és lemmák kimondását igényli.

4.10. Definíció. H hipergráfra $\tau(H)$ jelöli a hiperélek minimális számát amikkel lefedhető H összes csúcsa.

4.11. Lemma. *Egy r-uniform, d-reguláris H hipergráfra (azaz amiben minden él r csúcsot tartalmaz, és minden csúcsot d él fed le)*

$$\tau(H) \leq \frac{|V(H)|}{r} \ln |V(H)|$$

Bizonyítás. Legyen $|V(H)| = n$. Minden csúcsot d él fed le, és ezzel minden élet r-szer számolunk, így $|E(H)| = \frac{d}{r}n$ hiperéle van H-nak.

H hiperélei közül egyenletes eloszlás szerint egymástól függetlenül kiválasztunk k hiperélet (egy élet így akár többször is választhatunk).

Annak a valószínűsége, hogy egy adott csúcsot lefed egy adott véletlenszerűen kiválasztott él, az $\frac{d}{|E(H)|} = \frac{r}{n}$.

Tehát annak a valószínűsége, hogy egy adott csúcsot a k kisorsolt él egyike sem fed le, az $(1 - \frac{r}{n})^k$.

Ha $k \geq \frac{n}{r} \ln n$, akkor

$$(1-\frac{r}{n})^k = \left(\left(1-\frac{r}{n}\right)^{\frac{n}{r}}\right)^{\ln n} < \left(\frac{1}{e}\right)^{\ln n} = \frac{1}{n}$$

Ekkor a lefedetlen csúcsok számának várható értéke kisebb mint $n \cdot \frac{1}{n} = 1$, vagyis létezik k olyan hiperél, ami minden csúcsot lefed, azaz $\tau(H) \leq k$, vagyis

$$\tau(H) \leq \frac{|V(H)|}{r} \ln |V(H)|$$

□

4.12. Megjegyzés. Ennél egy erősebb állítás is igaz, valójában

$$\tau(H) \leq (1 + \log r)\frac{|V(H)|}{r},$$

azonban a jelen bizonyításunkhoz a gyengébb állítás is elég, és ezt a bizonyítástt szebbnek ítéltem.

Kimondjuk még az alábbi technikai lemmát, ami a bizonyítás során hasznos lesz:

4.13. Lemma (Iker-partíció). *[14]*
Adott egy Q véges halmaz, és két partíciója, S és T. Ekkor léteznek ezeknek a partícióknak S' és T' finomításai, hogy S' és T' osztályai bijekcióba állíthatók úgy, hogy a megfelelő osztályok azonos elemszámúak legyenek, és

$$|S'| = |T'| \leq |S| + |T|.$$

Bizonyítás. Az állítást $|S| + |T|$ szerinti indukcióval bizonyítjuk. $|S| + |T| = 2$ esetén az állítás világosan igaz, $S' = S = T = T' = Q$ jó megoldás.

Úgy fogjuk föl, mintha S és T két különböző, azonos elemszámú halmaznak, Q-nak és R-nek a partíciói lennének. Ez ekvivalens marad az eredeti állítással, ugyanúgy két egymással bijekcióba állítható finomított partíciót kell késztenünk.

Veszünk egy halmazt S-ből és egyet T-ből, az általánosság rovása nélkül az S-ből választott A halmaz elemszáma kisebb-egyenlő, mint a T-ből választott B halmazé.

Ekkor S-ből elhagyjuk az A halmazt, T-ben pedig a B halmaz elemszámát csökkentjük $|A|$-val. (Ha $|A| = |B|$, akkor ez azt jelenti, hogy B-t is elhagyjuk T-ből.)

Az így kapott partíciók továbbra is azonos, $|Q| - |A|$ elemszámú halmazok partíciói, és $|S| + |T|$ legalább 1-gyel csökkent, mert S-ből elhagytunk egy halmazt. Tehát indukció szerint léteznek legfeljebb $|S|+|T|-1$ méretű, bijekcióba állítható finomítások ezekhez. Ezekhez a finomításokhoz még hozzávesszük A-t, illetve B-nek az $|A|$ elemű elhagyott részét, és ez az eredeti partícióknak egy legfeljebb $|S|+|T|$ tagú, bijekcióba állítható finomításait adja. Ezzel az indukciós lépést beláttuk.

□

4.4. Központi tétel bizonyítása

Újra kimondjuk a központi tételt:

4.14. Tétel. *$\mathcal{F}$ és $\mathcal{G}$ irányított gráfok családjai egy közös X csúcshalmazon. Minden X-en értelmezett P eloszlásra*

$$C(\mathcal{F} \cup \mathcal{G}, P) \geq \min\{C(\mathcal{F}, P), C(\mathcal{G}, P)\}$$

Bizonyítás. Legyen $P_1, P_2, ...$ eloszlások egy sorozata, ami P-hez tart abban az értelemben, hogy

$$\max_{x \in X} |P_n(x) - P(x)| \to 0,$$

és $A_n \subset T_{P_n}$ és $B_n \subset T_{P_n}$ maximális szimmetrikus klikkek $\mathcal{F}$ illetve $\mathcal{G}$ szerint ezen a típuson belül.

A 4.6 Lemma bizonyítása ugyanúgy működik gráfcsaládokra is, így

$$\lim_{n\to\infty} \frac{1}{n} \log |A_n| = C(\mathcal{F}, P), \qquad \lim_{n\to\infty} \frac{1}{n} \log |B_n| = C(\mathcal{G}, P)$$

Ha π az n elemű halmaz egy permutációja, akkor $\pi(x)$ az $x = (x_1, ..., x_n)$ vektor elemeinek megfelelő permutációja, és az alábbi jelölést használjuk:

$$\pi(A_n) = \{\pi(x) | x \in A_n\}$$

Vegyük azt a hipergráfot, aminek a csúcsai T_{P_n} elemei, és a hiperélei a $\pi(A_n)$ halmazok az összes különböző permutációra. (Vegyük észre, hogy $A_n \subset T_{P_n}$, és ha $x \in T_{P_n}$, akkor $\pi(x) \in T_{P_n}$, így minden permutációra $\pi(A_n) \subset T_{P_n}$.)

A 4.11 Lemma szerint létezik $S_n^* \subset S_n$ (ahol S_n az n elemű halmaz permutációit jelöli), amire

$$\bigcup_{\pi \in S_n^*} \pi(A_n) = T_{P_n}, \qquad |S_n^*| \leq \frac{|T_{P_n}|}{|A_n|} \log |T_{P_n}|$$

Az unió diszjunkttá tehető, azaz választhatók egymástól diszjunkt $Q_\pi \in \pi(A_n)$ halmazok minden $\pi \in S_n^*$-ra, amiknek az uniója kiteszi T_{P_n}-et.

Ugyanígy létezik $S_n^{**} \subset S_n$, amire

$$\bigcup_{\pi \in S_n^{**}} \pi(B_n) = T_{P_n}, \qquad |S_n^{**}| \leq \frac{|T_{P_n}|}{|B_n|} \log |T_{P_n}|$$

Mint az előbb, itt is vehetünk egymástól diszjunkt $R_\pi \subset \pi(B_n)$ halmazokat, amiknek az uniója kiteszi T_{P_n}-et.

Most használjuk a 4.13 Lemmát.

Eszerint létezik egy $C_1 \cup ... \cup C_t$ és egy $D_1 \cup .... \cup D_t$ diszjunkt partíciói T_{P_n}-nek, amikben minden C_i egy Q_π és mindn D_i egy R_π részhalmaza, és $|C_i| = |D_i|$ minden $1 \leq i \leq t$-re és

$$t \leq 2\max\{\frac{|T_{P_n}|}{|A_n|}\log|T_{P_n}|, \frac{|T_{P_n}|}{|B_n|}\log|T_{P_n}|\}.$$

Mivel A_n és B_n szimmetrikus klikkek voltak $\mathcal{F}$ illetve $\mathcal{G}$ szerint, ezért egy adott permutációra $\pi(A_n)$ és $\pi(B_n)$ is szimmetrikus klikkek, mivel két vektorra a permutációtól megmarad az a tulajdonság, hogy van olyan koordináta, amiben az egyikből fut él a másikba, és van olyan, amiben a másikból az egyikbe.

Tehát a $C_i \subset Q_\pi \subset \pi(A_n)$ halmazok szimmetrkikus klikkek $\mathcal{F}$ szerint és a $D_i \subset R_\pi \subset \pi(B_n)$ halmazok szimmetrikus klikkek $\mathcal{G}$ szerint.

mn hosszú vektorokból képezünk egy szimmetrikus klikket $\mathcal{F} \cup \mathcal{G}$-re. (Az m számot később határozzuk meg.)

Csak olyan vektorokat vizsgálunk, amik m darab n hosszú szakaszból állnak, és minden szakaszuk T_{P_n}-ben van, és mostantól $x_1...x_m$ alakban jelenítjük meg ezeket a vektorokat, ahol minden $x_i \in T_{P_n}$.

4.15. Definíció. Definiáljuk az M halmazt, amiben az ilyen vektorok közül azok vannak, amikre ez a tulajdonság teljesül: minden $1 \leq i < m$-re igaz, hogy ha $x_i \in C_j$, akkor $x_{i+1} \in D_j$.

Továbbá tetszőleges $y \in T_{P_n}$ és $z \in T_{P_n}$ mellett definiáljuk az $M(y, z)$ halmazt, ami azon M-beli vektorok halmaza, amiknek az első szakasza y, és az m-edik szakasza z.

Belátjuk, hogy $M(y, z)$ mindig szimmetrikus klikk $\mathcal{F} \cup \mathcal{G}$ szerint, azaz szimmetrikus klikk $\mathcal{F}$ és $\mathcal{G}$ szerint is.

Vegyünk ugyanis két elemet $M(y, z)$-ből: $x_1x_2...x_m$ és $w_1w_2...w_m$ vektorokat. Mivel $x_1 = w_1 = y$, ezért létezik egy első olyan $i > 1$, amire $x_i \neq w_i$. Ekkor $x_{i-1} = w_{i-1}$, ami valamelyik C_j-be tartozik a partícióban. Ekkor M definíciója szerint x_i és w_i is D_j-be tartoznak, de különbözőek, így $\mathcal{G}$ minden eleme szerint mindkét irányba él fut a két vektor között, mivel D_j egy szimmetrikus klikk $\mathcal{G}$ szerint.

Hasonlóan, $x_m = w_m$, tehát létezik egy utolsó $i < m$, amire $x_i \neq w_i$. Ekkor $x_{i+1} = w_{i+1} = z$, amik a partícióban valamelyik D_j-be tartoznak, ekkor M definíciója szerint x_i-nek és w_i-nek is C_j-be kell esnie, és $x_i \neq w_i$, így a két vektor között mindkét irányba él fut $\mathcal{F}$ minden elemében, mivel C_j egy szimmetrikus klikk $\mathcal{F}$ szerint.

Ezzel beláttuk, hogy $M(y, z)$ egy szimmetrikus klikket képez $\mathcal{F} \cup \mathcal{G}$ szerint.

Mivel ez minden $y, z \in T_{P_n}$-re igaz, vehetjük azt a párt, amire $M(y, z)$ mérete a legnagyobb, ez legalább $\frac{|M|}{|T_{P_n}|^2}$. Már csak $|M|$ méretét kell tehát megbecsülnünk.

Itt segítségünkre lesz néhány alapvető információelméleti állítás az entrópiáról, amiket korábban bemutattunk.

Veszünk egy valószínűségi eloszlást M-ben lévő $X_1X_2...X_m$ sorozatokon az alábbi módon: az X_1 szakaszt egyenletes valószínűséggel sorsoljuk T_{P_n}-ből, ezután mindig megnézzük, hogy az X_i szakasz a partíció melyik C_j halmazába esik, és X_{i+1}-et egyenletes valószínűséggel választjuk D_j elemei közül.

Ekkor a 2.4 Tétel szerint

$$H(X_1, X_2, ..., X_m) \le \log |M|,$$

továbbá az 2.7 tétel szerint az entrópia felbontható feltételes entrópiák összegére, azaz

$$H(X_1, X_2, ..., X_m) = H(X_1)+H(X_2|X_1)+H(X_3|X_1, X_2)+...+H(X_m|X_1, X_2, ..., X_{m-1})$$

Mivel X_i kisorsolása csak X_{i-1}-től függ, ezért

$$H(X_i|X_1, X_2, ..., X_{i-1}) = H(X_i|X_{i-1}).$$

Továbbá indukcióval beláthajuk, hogy minden X_i egyenletes eloszlású T_{P_n}-en: X_1 valóban egyenletes eloszlású, és utána tetszőleges j-re $x \in D_j$-re

$$P(X_i = x) = \frac{1}{|D_j|} \sum_{y \in C_j} P(X_{i-1} = y) = \frac{1}{|D_j|} \frac{|C_j|}{|T_{P_n}|} = \frac{1}{|T_{P_n}|},$$

mivel úgy hoztuk létre a partíciókat, hogy $|C_j| = |D_j|$.

Tehát minden $H(X_i|X_{i-1})$ annak az entrópiája, hogy X_{i-1}-et egyenletesen kisorsoljuk T_{P_n}-en, aztán aszerint szabályszerűen kisorsoljuk X_i-t. Vagyis ezek az entrópiák mind egyenlők $H(X_2|X_1)$-gyel, továbbá $H(X_1) = H(X_2) \ge H(X_2|X_1)$, tehát

$$H(X_1, X_2, ..., X_m) \ge mH(X_2|X_1).$$

A definíció alapján megbecsüjük $H(X_2|X_1)$-et:

$$H(X_2|X_1) = \sum_{j=1}^{t} \frac{|C_j|}{|T_{P_n}|} \log |C_j|$$

A konvex $x \log x$ függvényre alkalmazott Jensen-egyenlőtlenség szerint (lásd 2.5 Lemma)

$$H(X_2|X_1) = \sum_{j=1}^{t} \frac{|C_j|}{|T_{P_n}|} \log |C_j| \ge \frac{1}{|T_{P_n}|} \left(\sum_{j=1}^{t} |C_j| \right) \log \frac{\sum_{j=1}^{t} |C_j|}{t} = \log \frac{|T_{P_n}|}{t}$$

Tudjuk, hogy

$$t \le 2 \max\{\frac{|T_{P_n}|}{|A_n|} \log |T_{P_n}|, \frac{|T_{P_n}|}{|B_n|} \log |T_{P_n}|\},$$

tehát

$$H(X_2|X_1) \geq \log \min\{\frac{|A_n|}{2\log|T_{P_n}|}, \frac{|B_n|}{2\log|T_{P_n}|}\}.$$

Legyen $m = n$. Ekkor

$$\log|M(y,z)| \geq \log\frac{|M|}{|T_{P_n}|^2} \geq n\log\min\{\frac{|A_n|}{2\log|T_{P_n}|}, \frac{|B_n|}{2\log|T_{P_n}|}\} - 2n\log|X|,$$

mivel $\log|M| \geq nH(X_2|X_1)$ és $|T_{P_n}| \leq |X|^n$.

$\log|T_{P_n}| \leq n\log|X|$, így

$$\log|M(y,z)| \geq n\log\min\{|A_n|, |B_n|\} - n\log(2n\log|X|) - 2n\log|X|.$$

$M(y,z)$ elemei n^2 hosszú vektorok, és mint már beláttuk, $M(y,z)$ szimmetrikus klikket alkot $\mathcal{F}\cup\mathcal{G}$ szerint. Továbbá minden $M(y,z)$-beli vektor T_{P_n}-beli vektorok egymás után fűzése, így maguk az $M(y,z)$-beli vektorok is a T_{P_n} típushoz tartoznak, és P_n eloszlások tartanak P-hez, így definíció szerint

$$C(\mathcal{F}\cup\mathcal{G}, P) \geq \limsup_{n\to\infty}\frac{1}{n^2}\log|M(y,z)| \geq \limsup_{n\to\infty}\frac{1}{n}\log\min\{|A_n|, |B_n|\},$$

a többi tag ugyanis 0-hoz tart az n^2-tel leosztás után.

$$\limsup_{n\to\infty}\frac{1}{n}\log\min\{|A_n|, |B_n|\} = \min\{\limsup_{n\to\infty}\frac{1}{n}\log|A_n|, \limsup_{n\to\infty}\frac{1}{n}\log|B_n|\} = \min\{C(\mathcal{F}, P), C(\mathcal{G}, P)\}.$$

Ezzel a központi tételt beláttuk.

□

4.5. Élek gráfcsaládjának kapacitása

Hogy jobban megértsük a Gargano-Körner-Vaccaro-tételt, rögtön meghatározzuk vele bizonyos egszerű, de fontos gráfcsaládok Sperner-kapacitását.

4.16. Definíció. Egy n csúcsú G egyszerű gráfra $\mathcal{G}(G)$-vel jelöljük azt a családot, amit úgy kapunk, hogy G minden élét belevesszük egy egy-élű irányított gráfként tetszőleges irányítással.

4.17. Tétel (Greco)**.** *[4]*

$C(\mathcal{G}(G)) = \frac{2}{n}$ pontosan akkor teljesül, ha G csúcsai lefedhetők csúcsdiszjukt élek és páratlan körök uniójával.

Ebből azonnal következik például az a hasznos speciális eset, hogy ha G a teljes gráf, azaz $\mathcal{G}(G)$-ben az összes egyélű irányított gráf szerepel, akkor $C(\mathcal{G}(G)) = \frac{2}{n}$.

A tétel bizonyításához először belátjuk az alábbi tételt:

4.18. Tétel. *Ha G egy irányított gráf az X csúcshalmazon, és egyetlen irányított ab éle van, és P egy valószínűségi eloszlás X-en, amire $P(a)$ és $P(b)$ legalább egyike nem 0, akkor*

$$C(G,P) = (P(a)+P(b))h\left(\frac{P(a)}{P(a)+P(b)}\right),$$

ahol $h(p)$ a bináris entrópia függvény, azaz

$$h(p) = -p\log p - (1-p)\log(1-p).$$

Bizonyítás. Legyen P_n egy lehetséges eloszlás az n-hosszú vektoron, úgy, hogy $P_1, P_2, ...$ konvergál P-hez.

Legyen C_n olyan T_{P_n}-beli vektorok halmaza, amiknek az első $n(P_n(a)+P_n(b))$ eleme a vagy b, és minden ilyen kezdőszelethez pontosan egy C_n-beli vektor tartozik. Ekkor C_n szimmetrikus klikket alkot G^n-ben, ugyanis bármely két vektorra van olyan koordináta az első $n(P_n(a)+P_n(b))$ között, ahol egyik a és a másik b, és olyan koordináta is, ahol fordítva.

$$|C_n| = \binom{n(P_n(a)+P_n(b))}{nP_n(a)},$$

ezért, felhasználva a 4.3 lemma egy speciális esetét kételemű ábécére:

$$C(G,P) \geq \limsup_{n\to\infty} \frac{1}{n}\log\binom{n(P_n(a)+P_n(b))}{nP_n(a)} = (P(a)+P(b))h\left(\frac{P(a)}{P(a)+P(b)}\right).$$

Bizonyítsuk most a másik irányú egyenlőtlenséget:

Legyen T_Q az n-hosszú vektorok egy tetszőleges típusa, és legyen $D \subset T_Q$ egy szimmetrikus klikk G^n-ben.

Egy $x_i \in D$ n-hosszú vektorhoz hozzárendeljük az $\{1,2,...,n\}$ halmaz A_i és B_i részhlamazait, amik az x_i vektorban az a illetve b elemek elhelyezkedését mutatják.

Az, hogy az x_i vektorok szimmetrikus klikket alkotnak G^n-ben, azzal ekvivalens, hogy az A_i és B_i halmazok úgynevezett Bollobás-párokat alkotnak, azaz tetszőleges $i \neq j$-re $A_i \cap B_j \neq \emptyset$, viszont minden i-re $A_i \cap B_i = \emptyset$.

4.19. Lemma. *[3]*

Ha $i = 1, 2..., k$-ra A_i és B_i Bollobás-párok egy n elemű alaphalmazon, akkor teljesül, hogy

$$\sum_{i=1}^{k} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} \leq 1$$

Bizonyítás. Minden (A_i, B_i) párra vesszük az $[n]$ halmaz összes olyan permutációját, amiben A_i minden eleme megelőzi B_i minden elemét.

Az ilyen permutációk száma

$$|A_i|!|B_i|!\binom{n}{|A_i|+|B_i|}(n-|A_i|-|B_i|)!$$

A különböző i értékekre így a permutációk diszjunkt halmazait kapjuk az $A_i \cap B_j \neq \emptyset$ tulajdonság miatt. Tehát

$$\sum_{i=1}^{k} |A_i|!|B_i|!\binom{n}{|A_i|+|B_i|}(n-|A_i|-|B_i|)! \leq n!$$

Átrendezve megkapjuk, hogy

$$1 \geq \sum_{i=1}^{k} \frac{|A_i|!|B_i|!}{(|A_i|+|B_i|)!} = \sum_{i=1}^{k} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}}$$

□

Innen már könnyű befejezni a tétel bizonyítását:

A $D \subset T_Q$ szimmetrikus klikk minden elemére $|A_i| = nQ(a)$ és $|B_i| = nQ(b)$, ezért az előző lemma szerint

$$\sum_{x \in D} \frac{1}{\binom{n(Q(a)+Q(b))}{nQ(a)}} \leq 1,$$

vagyis

$$|D| \leq \binom{n(Q(a)+Q(b))}{nQ(a)}.$$

Ha P_n eloszlások tartanak P-hez, és $D_n \subset T_{P_n}$ a maximális szimmetrikus klikk $G^n[P_n, 0]$-ban, akkor a 4.6 Lemma szerint

$$\lim_{n\to\infty} \frac{1}{n} \log |D_n| = C(G, P),$$

amiből az előző szerint következik, hogy

$$C(G, P) \leq \lim_{n\to\infty} \frac{1}{n} \log \binom{n(P_n(a)+P_n(b))}{nP_n(a)} = (P(a)+P(b))h\left(\frac{P(a)}{P(a)+P(b)}\right)$$

□

4.20. Megjegyzés. Érdemes megjegyezni, hogy a felső becslésre adott bizonyítással az is megmutatható, hogy ha $P(a) = 0$ és $P(b) = 0$, akkor $C(G, P) = 0$.

Most rátérhetünk a 4.17 Tétel bizonyítására:

Bizonyítás. A 4.8 Tétel és az imént bizonyított 4.18 Tétel egyesítésből azt kapjuk, hogy

$$C(\mathcal{G}(G)) = \max_P \min_{(u,v)\in E(G)} (P(a) + P(b))h\left(\frac{P(a)}{P(a) + P(b)}\right)$$

Ha minden csúcsra $\frac{1}{n}$ súlyt írunk, akkor minden élre

$$(P(a) + P(b))h\left(\frac{P(a)}{P(a) + P(b)}\right) = \frac{2}{n},$$

tehát tetszőleges nem-üres G gráfra

$$C(\mathcal{G}(G)) \geq \frac{2}{n}.$$

Tegyük föl, hogy G csúcsai lefedhetők diszjunkt élekkel és páratlan körökkel. Ekkor tetszőleges P eloszlás mellett létezik olyan él vagy páratlan kör a lefedésben, hogy a benne lévő csúcsokon az átlagos súly legfeljebb $\frac{1}{n}$. Ekkor ebben van olyan él, amin a súlyok összege legfeljebb $\frac{2}{n}$, és ismert, hogy $h(p) \leq h(\frac{1}{2}) = 1$, így erre az élre

$$(P(a) + P(b))h\left(\frac{P(a)}{P(a) + P(b)}\right) \leq \frac{2}{n}.$$

Ezzel beláttuk, hogy az olyan gráfokra, amik lefedhetők csúcsdiszjunkt élek és páratlan körök uniójával,

$$C(\mathcal{G}(G)) = \frac{2}{n}.$$

Tegyük föl, hogy a G gráfban van a csúcsoknak egy H halmaza, amikre teljesül, hogy H elemei között nem fut él, és a H-beliekkel szomszédos csúcsok száma kevesebb, mint $|H|$.

Legyen $|H| = k$ és H szomszédainak elemszáma $t < k$. Ekkor H elemeire $\frac{1}{n} - \varepsilon$ súlyt írunk, H szomszédaira pedig $\frac{1}{n} + \frac{k-\frac{1}{2}}{t}\varepsilon$ súlyt írunk.

Így a H-ból kifutó éleken

$$P(a) + P(b) = \frac{1}{n} - \varepsilon + \frac{1}{n} + \frac{k - \frac{1}{2}}{t}\varepsilon = \frac{2}{n} + \frac{k - t - \frac{1}{2}}{t}\varepsilon \geq \frac{2}{n} + \frac{\varepsilon}{2t}.$$

Mivel $h(\frac{1}{2}) = 1$ és $h'(0) = 0$, és

$$\frac{P(a)}{P(a) + P(b)} = \frac{\frac{1}{n} - \varepsilon}{\frac{2}{n} + \frac{k-t-\frac{1}{2}}{t}\varepsilon} \to \frac{1}{2}$$

ahogyan ε tart a 0-hoz, ezért kellően kicsi ε értékre

$$1 - h\left(\frac{P(a)}{P(a)+P(b)}\right) \leq \frac{\varepsilon}{5t},$$

ekkor

$$(P(a)+P(b))h\left(\frac{P(a)}{P(a)+P(b)}\right) \geq (\frac{2}{n} + \frac{\varepsilon}{2t})(1 - \frac{\varepsilon}{5t}) \geq \frac{2}{n}.$$

H csúcsaira és a szomszédaira összesen $k(\frac{1}{n} - \varepsilon) + t(\frac{1}{n} + \frac{k-\frac{1}{2}}{t}\varepsilon) = (k+t)\frac{1}{n} - \frac{1}{2}\varepsilon$ súlyt írtunk, így az összes többi $n-k-t$ csúcsra írhatunk $\frac{1}{n}$-nél nagyobb súlyt. Így minden olyan él, ami nem H egy eleméből indul ki, két olyan csúcsot köt össze, amiken $\frac{1}{n}$-nél nagyobb súly van.

$$(P(a)+P(b))h\left(\frac{P(a)}{P(a)+P(b)}\right) = (P(a)+P(b))\log(P(a)+P(b)) - P(a)\log P(a) - P(b)\log P(b),$$

ennek a $P(a)$ szerinti deriváltja

$$\log(P(a)+P(b)) - \log P(a) > 0,$$

tehát $P(a)$ növelésével nő az érték, ugyanez igaz $P(b)$-re. Tehát ha $P(a) > \frac{1}{n}$ és $P(b) > \frac{1}{n}$, akkor

$$(P(a)+P(b))h\left(\frac{P(a)}{P(a)+P(b)}\right) > \frac{2}{n}.$$

H-t úgy választottuk, hogy nincs olyan él, amelynek mindkét csúcsa H-ban van, ezzel tehát az összes élt megvizsgáltuk.

Ebből az következik, hogy ha egy gráfra $C(\mathcal{G}(G)) \leq \frac{2}{n}$, az csak úgy lehetséges, ha nincsen benne ilyen H független csúcshalmaz, amelynek $|H|$-nál kevesebb szomszédja van.

Ekkor viszont létezik a csúcsoknak fedése diszjunkt élekkel és páratlan körökkel. Ezt az állítást Tutte-tételnek nevezeik, és mi itt az alábbi, a magyar módszeren alapuló algoritmus segítségével bizonyítjuk:

Tegyük föl, hogy néhány diszjunkt élt és páratlan kört már berajzoltunk a gráfba, de még nem minden csúcsot fedtünk le.

Legyen v egy lefedetlen csúcs. Célunk, hogy úgy módosítsuk a diszjunkt élekkel és páratlan körökkel való lefedést, hogy minden eddig fedett csúcs fedve maradjon, és v is le legyen fedve.

Létre fogunk hozni egy H és egy R csúcshalmazt. Tekintsük a v-ből induló alternáló utakat, azaz az olyan utakat, amiknek az élei felváltva diszjunkt élek az eddigi fedésben, és olyan élek, amik nem szerepeltek az eddigi fedésben. Legyen H az olyan pontok halmaza, melyek v-ből (élszám szerint) páros hosszú alternáló úton érhetők el, R pedig az olyan pontok halmaza, melyek v-ből páratlan hosszú alternáló úton érhetők el. Vegyük észre, hogy ha H-nak és R-nek van közös eleme, akkor az ide vezető alternáló utak egyesítését tekintve lehet találni egy páratlan kört, melybe v-ből páros hosszú út vezet, és akkor a páratlan kört be lehet venni a benne szereplő diszjunkt élek helyett, míg a páros úton meg lehet cserélni a kiválasztott élek paritását, így v is bekerül a fedésbe.

Ha R-be egy olyan w csúcs kerül, amely nincs lefedve, akkor megtehetjük, hogy ehelyett az út másik paritású éleit vesszük be a lefedésbe, így az út közbülső csúcsai továbbra is lefedettek maradnak, és v és w is lefedésre kerülnek.

Ha R-be egy olyan w csúcs kerül, amely az eddigi lefedésben egy páratlan körben szerepelt, akkor mivel $v \in H$ és $w \in R$, ezért a v-ből w-be vezető alternáló útnak w nélkül páratlan csúcsa van, ezért az alternáló útnak és a w-t tartalmazó páratlan körnek együtt páros sok csúcsa van, így együtt felbonthatók v-t is lefedő diszjunkt élekre. (Ekkor tehát a páratlan kört elhagyjuk a lefedésből.)

Ha két H-ban lévő w és z csúcs szomszédos a gráfban, akkor megkeressük a legkésőbbi közös ősüket az algoritmus szerint H-n belül, legyen ez a q csúcs. q-ból w-be és q-ból z-be is páros hosszú alternáló út vezet, ehhez még hozávesszük a wz élt, és az így kapott páratlan kör része lesz az új lefedésünknek. Emellett a v-ből q-ba vezető alternáló útban is lecserélhetjük, hogy milyen paritású éleket veszünk be, ezzel v is a fedés része lesz, az út közbülső csúcsai fedve maradnak, és bár q-t így nem fedi diszjunkt él, azt szerencsére már fedi az új páratlan kör.

Tehát ha v-t nem tudjuk hozzávenni a fedéshez, az csak úgy lehetséges, ha R minden elemének van párja egy diszjunkt élen keresztül H-ban, és H-n belül nem fut él. Ekkor H-ban szerepel v, és H összes többi csúcsát úgy kaptuk, mint egy R-beli csúcs párja, tehát H-ban eggyel több csúcs van, mint R-ben, és H összes szomszédja már R-ben van, különben nem állt volna még meg az algoritmus.

Azonban ha $C(\mathcal{G}(G)) = \frac{2}{n}$, akkor beláttuk, hogy ilyen H csúcshalmaz nem létezhet, tehát ha $C(\mathcal{G}(G)) = \frac{2}{n}$, akkor minden fedéshez hozzávehető egy kimaradó v csúcs, így létezik teljes fedés diszjunkt élekkel és páratlan körökkel.

Ezzel az ekvivalenciát beláttuk.

□

5. Witsenhausen-ráta

Az előzőekhez hasonló információküldési probléma a következő:

A forrás V betűhalmazából egy X valószínűségi változót figyel meg az adó, ezt kell továbbítania k különböző vevőnek.

Minden vevőnek van egy mellékinformációja: az i-edik vevő megfigyel egy Y_i valószínűségi változót, amely függhet X-től. Az adó nem tudja, milyen Y_i értékeket kaptak a vevők, csak a valószínűségi mátrixot ismeri, hogy milyen X mellett milyen valószínűséggel jelennek meg az egyes értékek Y_i-ként.

A Witsenhausen-ráta az, hogy kellően nagy blokk-kódokat használva, érkező betűnként átlagosan hány bit elküldésére van szükség ahhoz, hogy minden vevő biztosan dekódolni tudja a forrásból érkező X betűket.

Érdemes megjegyezni, hogy ez egy úgynevezett forráskódolási feladat, nem pedig csatornakódolási, amikkel eddig foglalkoztunk. Így ez a ráta bizonyos értelemben ellentétes kapcsolatban áll a korábban vizsgált kapacitásokkal: míg korábban az volt a kérdés, átlagosan hány betűnyi üzenet küldhető el bitenként, itt az a kérdés, hogy hány bit kell egy betűnyi információ elküldéséhez.

Minden i vevőhöz hozzárendeljük a G_i gráfot a V csúcshalmazon, amiben a V-beli v_1 és v_2 betűk akkor vannak összekötve, ha az i-edik vevő számára összetéveszthetőek lehetnek, azaz ha létezik olyan b érték, hogy

$$P(Y_i = b|X = v_1) > 0, \qquad P(Y_i = b|X = v_2) > 0$$

Fontos megjegyezni, hogy ez a G gráf az eddig vizsgált gráfok komplementereként tekinthető:

A Shannon- és Sperner-kapacitások vizsgálatánál akkor kötöttünk össze két csúcsot, ha összetéveszthetetlenek voltak, most pedig akkor ha összetéveszthetőek. Ez egy visszatérő kettősség a szakirodalomban, ugyanis különböző helyzetekben más definíció a kézenfekvő: a Sperner-kapacitásnál bevezetett irányított gráfokat úgy lehetett jól kezelni, itt pedig hamarosan látni fogjuk, miért kényelmesebb a komplementerrel dolgozni.

A G^n gráfot is az előzőekben bevezetett hatvány komplementereként definiáljuk:

Most G^n-ben csúcsok vektorai akkor vannak összekötve, ha minden koordinátában vagy megegyeznek, vagy összekötött csúcsok szerepelnek bennük.

Ezzel a komplementer definícióval dolgozva újra definiáljuk a $C_{AND}(G, P)$ kapacitásértéket.

(Az elnevezés onnan származik, hogy ennél a gráfhatványozásnál minden koordinátában teljesülnie kell valaminek, míg a korábbi gráfhatványozási definícióban az kellett, hogy legalább egy helyen teljesüljön valami. Így a korábbi $C(G)$ fogalmat $C_{OR}(G)$-vel is jelölhettük volna.)

5.1. Definíció.

$$C_{AND}(G, P) = \lim_{\delta \to 0} \limsup_{n \to \infty} \frac{1}{n} \log \alpha(G^n[P, \delta])$$

ahol α a gráf függetlenségi számát jelöli. Mivel egy gráf függetlenségi száma a maximális klikk mérete a komplementerében, ez a kapacitás fogalom ugyanaz, mint az eddigi, csak az új gráfhatványozási definíció mellett.

Most definiálhatjuk egzaktul egy gráf Witsenhausen-rátáját:

5.2. Definíció. [15]

Egy G egyszerű gráf Witsenhausen-rátája

$$R(G) = \lim_{n \to \infty} \frac{1}{n} \log \chi(G^n).$$

Ez azt fejezi ki, hogy ha az adónak meg kell ismertetnie a vevővel X-et, és a kettejükhöz tartozó összekeverhetőségi gráf G, akkor n hosszú szavak küldésekor V^n két eleme pontosan akkor kaphatja ugyanazt a kódszót, ha a vevő számára nem lehetnek összetéveszthetőek, vagyis ha a G^n gráfban nem összekötöttek. Ha a kódszavakat színeknek feleltetjük meg, akkor a minimálisan szükséges kódszavak száma éppen $\chi(G^n)$.

(Ezért használjuk ebben a részben a komplementer gráfot, a kromatikus számnak megfelelő klikk-lefedési szám egy kevésbé természetes fogalom.)

5.3. Definíció. Ha k vevő van, és a hozzájuk tartozó G_i gráfok halmazát $\mathcal{G}$-vel jelöljük, akkor a $\mathcal{G}$ gráf-család Witsenhausen-rátája

$$R(\mathcal{G}) = \lim_{n\to\infty} \frac{1}{n} \log \chi(\cup_{G\in\mathcal{G}} G^n).$$

Ugyanis ha az adó azt akarja, hogy minden vevő dekódolni tudja az üzenetet, akkor két V^n-beli szó csak akkor kaphatja ugyanazt a kódot, ha semelyik G_i^n szerint nincsenek összekötve, azaz a kódszavak $\cup_i G_i^n$ egy színezését adják.

A korábban bevezetett $C(\mathcal{G}, P)$ és $C(\mathcal{G}, P)$ fogalmakkal analóg módon egy V-n értelmezett P valószínűségi eloszlás esetén bevezetjük a típuson belüli rátákat:

5.4. Definíció.

$$R(G, P) = \lim_{\delta\to 0} \limsup_{n\to\infty} \frac{1}{n} \log \chi(G^n[P, \delta])$$

és

$$R(\mathcal{G}, P) = \lim_{\delta\to 0} \limsup_{n\to\infty} \frac{1}{n} \log \chi(\cup_{G\in\mathcal{G}} G^n[P, \delta])$$

A Witsenhausen-rátáról szóló fő tételünk Marton Katalin egy tételének általánosabban kimondott verzióján alapul:

5.5. Lemma (Marton lemmája)**.** *[8]*

$$R(\mathcal{G}, P) = H(P) - C_{AND}(\mathcal{G}, P)$$

Ennek egy egyszerű következménye $\mathcal{G} = \{G\}$-re az alábbi álltás:

5.6. Következmény.

$$R(G, P) = H(P) - C_{AND}(G, P)$$

Eredetileg csak ezt a következményt mondta ki Marton Katalin, de mivel a bizonyítás megyegyezik, a gráfcsaládos 5.5 Lemmára is Marton lemmájaként hivatkozunk.

Az 5.5 Lemma bizonyításhoz be kell vezetnünk a tört-kromatikus szám fogalmát.

5.7. Definíció. A G gráf minden független S csúcshalmazásához hozzárendelünk egy $f(S)$ súlyt úgy, hogy tetszőleges x csúcsra

$$\sum_{S \ni x} f(S) \geq 1.$$

Az ilyen f súlyozásokat nevezzük tört-színezésnek, és G tört-kromatikus száma

$$\chi^*(G) = \min_f \sum_S f(S),$$

ahol S az összes független csúcshalmazon fut végig, f pedig a lehetséges tört-színezéseken.

Észrevehetjük, hogy egy $\chi(G)$ színből álló színezés esetén helyes tört-színezés az, ha minden c szín esetén a c színű csúcsok halmaza (ami egy független csúcshalmaz) 1 súlyt kap, és minden más független csúcshalmaz 0 súyt kap. Ekkor ugyanis minden x csúcs pontosan egy színhez tartozik, így pontosan egy olyan S halmazban van, aminek 1 a súlya, tehát $\sum_{S \ni x} f(S) = 1$.
Erre a tört-színezésre $\sum\limits_S f(S) = \chi(G)$, ebből az következik, hogy

$$\chi^*(G) \leq \chi(G).$$

Lovász egy tétele másik irányú becslést is ad:

5.8. Lemma. *[6]*

$$\chi^*(G) \geq \frac{\chi(G)}{1 + \ln \alpha(G)}$$

Megfigyelhető továbbá az alábbi összefüggés:

5.9. Lemma. *Egy csúcstranzitív G gráfra*

$$\chi^*(G) = \frac{|V(G)|}{\alpha(G)}$$

Bizonyítás. Általános G gráfra teljesül, hogy

$$|V(G)| \leq \sum_{v \in V} \sum_{S \ni v} f(S) = \sum_S |S| f(S) \leq \alpha(G) \sum_S f(S) = \alpha(G)\chi^*(G),$$

tehát

$$\chi^*(G) \geq \frac{|V(G)|}{\alpha(G)}.$$

Ha a G gráf csúcs-tranzitív, akkor vehetjük azt a súlyozást, amiben minden $\alpha(G)$ méretű független halmaz c súlyt kap, a többi független halmaz 0-t.

Mivel a gráf csúcs-tranzitív, minden csúcsot ugyanannyi, k darab $\alpha(G)$ méretű független halmaz tartalmaz. Ekkor legyen $c = \frac{1}{k}$. Így valóban minden csúcsra az őt tartalmazó halmazok össz-súlya legalább 1.

Az $\alpha(G)$ elemszámú független halmazok száma legyen M, ekkor az ilyen halmazok és csúcsok illeszkedéseinek száma egyrészt $M\alpha(G)$, másrészt $k|V(G)|$, mert minden csúcsot k ilyen halmaz fed le.

Tehát $k|V(G)| = M\alpha(G)$, azaz $\frac{M}{k} = \frac{|V(G)|}{\alpha(G)}$.

A megadott súlyozás össz-súlya $M\frac{1}{k} = \frac{|V(G)|}{\alpha(G)}$, tehát egy csúcstranzitív G gráfra $\chi^*(G) \leq \frac{|V(G)|}{\alpha(G)}$.

Ebből együtt megkapjuk a Lemma állítását, miszerint egy csúcstranzitív G gráfra

$$\chi^*(G) = \frac{|V(G)|}{\alpha(G)}.$$

□

Most rátérhetünk a Witsenhausen-rátáról szóló 5.5 Lemma bizonyítására:

Bizonyítás. Legyen P_n eloszlások egy sorozata V-n, amik tartanak P-hez abban az értelemben, hogy

$$\lim_{n\to\infty} \max_{v\in V} |P(v) - P_n(v)| = 0.$$

Ekkor a 4.6 Lemmához nagyon hasonló bizonyítás adható arra, hogy

$$R(\mathcal{G}, P) = \lim_{n\to\infty} \frac{1}{n} \log \chi(\cup_{G\in\mathcal{G}} G^n[P_n, 0])$$

A $\cup_{G\in\mathcal{G}} G^n[P_n, 0]$ gráfot a kényelem kedvéért elnevezzük F_n-nek.

Lovász 5.8 lemmája szerint

$$\chi^*(F_n) \leq \chi(F_n) \leq \chi^*(F_n)(1 + \ln \alpha(F_n)).$$

$$\lim_{n\to\infty} \frac{1}{n} \log(1 + \ln \alpha(F_n)) \leq \lim_{n\to\infty} \frac{1}{n} \log(1 + n \ln |V|) = 0,$$

ezért

$$R(\mathcal{G}, P) = \lim_{n\to\infty} \frac{1}{n} \log \chi(F_n) = \lim_{n\to\infty} \frac{1}{n} \log \chi^*(F_n)$$

Mivel F_n csúcsai, azaz a T_{P_n}-ben lévő vektorok egymásból permutációval megkaphatók, és egy permutáció a vektorok elemein nem változtatja meg a szomszédságukat, ezért az F_n gráf csúcs-tranzitív.

Tehát az 5.9 Lemma szerint

$$\chi^*(F_n) = \frac{|V(F_n)|}{\alpha(F_n)} = \frac{|T_{P_n}|}{\alpha(F_n)}.$$

Vagyis

$$R(\mathcal{G}, P) = \lim_{n\to\infty} \frac{1}{n} \log \frac{|T_{P_n}|}{\alpha(F_n)}$$

A 4.3 Lemmából tudjuk, hogy

$$\lim_{n\to\infty} \frac{1}{n} \log |T_{P_n}| = H(P)$$

és definíció szerint

$$C_{AND}(\mathcal{G}, P) = \lim_{n\to\infty} \frac{1}{n} \log \alpha(F_n).$$

Ezzel valóban azt kaptuk, hogy

$$R(\mathcal{G}, P) = \lim_{n\to\infty} \frac{1}{n} \log \frac{|T_{P_n}|}{\alpha(F_n)} = H(P) - C_{AND}(\mathcal{G}, P).$$

□

Fontos még az alábbi állítást kimondanunk:

5.10. Lemma.

$$R(\mathcal{G}) = \max_P R(\mathcal{G}, P)$$

Bizonyítás. A bizonyítás szó szerint megegyezik a 4.7 Tétel bizonyításával.

□

Ezekből a lemmákból és a 4.8 Gargano-Körner-Vaccaro-tételből megkaphatunk egy, a gráfcsaládok Witsenhausen-rátájára vonatkozó alapvető tételt:

5.11. Tétel (Simonyi)**.** *[11]*
Ha $\mathcal{G}$ gráfok egy véges családja egy közös V csúcshalmazon, akkor

$$R(\mathcal{G}) = \max_{G\in\mathcal{G}} R(G)$$

Bizonyítás. Az 5.10 Lemma szerint

$$R(\mathcal{G}) = \max_P R(G, P).$$

Az 5.5 Marton-lemma szerint

$$\max_P R(G,P) = \max_P (H(P) - C_{AND}(\mathcal{G},P)).$$

A 4.8 Gargano-Körner-Vaccaro-tétel szerint

$$\max_P (H(P) - C_{AND}(\mathcal{G},P)) = \max_P (H(P) - \min_{G\in\mathcal{G}} C_{AND}(G,P)) = \max_P \max_{G\in\mathcal{G}} (H(P) - C_{AND}(G,P))$$

Az 5.6 Marton-lemma Következmény szerint

$$\max_P \max_{G\in\mathcal{G}} (H(P) - C_{AND}(G,P)) = \max_P \max_{G\in\mathcal{G}} R(G,P).$$

Az 5.10 Lemmát alakalmazva $\mathcal{G} = \{G\}$-re pedig azt kapjuk, hogy

$$\max_P \max_{G\in\mathcal{G}} R(G,P) = \max_{G\in\mathcal{G}} R(G)$$

Ezeket a lépéseket egymás után fűzve megkapjuk a kívánt állítást, miszerint

$$R(\mathcal{G}) = \max_{G\in\mathcal{G}} R(G)$$

□

Hivatkozások

[1] N. Alon. On the capacity of digraphs. *European Journal of Combinatorics*, 19:1–5, 1998.

[2] A. Blokhuis. On the Sperner capacity of the cyclic triangle. *Journal of Algebraic Combinatorics*, 2:123–124, 1993.

[3] B. Bollobás. On generalized graphs. *Acta Mathematica Academiae Scientiarum Hungaricae*, 16:445–452, 1965.

[4] G. Greco. Capacities of graphs and 2-matchings. *Discrete Mathematics*, 186:135–143, 1998.

[5] I. Csiszár , J. Körner. *Information Theory*. Cambridge University Press, 2011.

[6] L. Lovász. On the ratio of optimal integer and fractional covers. *Discrete Mathematics*, 13:383–390, 1975.

[7] L. Lovász. On the Shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25:1–7, 1979.

[8] K. Marton. On the Shannon capacity of probabilistic graphs. *Journal of Combinatorial Theory, Series B*, 57:183–195, 1993.

[9] C. E. Shannon. The zero-error capacity of a noisy channel. *IRE Transactions on Information Theory*, 2:8–19, 1956.

[10] A. R. Calderbank, P. Frankl, R. L. Graham, W.-C. W. Li, L. A. Shepp. The Sperner capacity of the cyclic triangle for linear and non-linear codes. *Journal of Algebraic Combinatorics*, 2:31–48, 1993.

[11] G. Simonyi. On Witsenhausen's zero-error rate for multiple sources. *IEEE Transactions on Information Theory*, 2004.

[12] J. Körner, C. Pilotto, G. Simonyi. Local chromatic number and Sperner capacity. *Journal of Combinatorial Theory, Series B*, 95:101–117, 2005.

[13] Schwarcz Tamás. Gráfok shannon-kapacitása, 2018.

[14] L. Gargano, J. Körner, U. Vaccaro. Capacities: from information theory to extremal set theory. *Journal of Combinatiorial Theory, Series A*, 68:296–315, 1994.

[15] H. S. Witsenhausen. The zero-error side-information problem and chromatic numbers. *IEEE Transactions on Information Theory*, 22:592–593, 1976.