Eötvös Loránd Tudományegyetem
Természettudományi Kar

Balázs Barbara Anna
Matematikus MSc.

Kódok kombinatorikus vonatkozásai

Szakdolgozat

Témavezető: Katona Gyula, egyetemi tanár
Számítógéptudományi Tanszék

Budapest, 2014.

Tartalomjegyzék

1. Bevezetés

A dolgozat azt a kérdést vizsgálja, hogy milyen kombinatorikus eszközök állnak rendelkezésünkre különféle kódelméleti problémák megoldásához. Az 1.1. alfejezetben megtalálható az összes olyan kódelméleti alapismeret, melyre szükségünk lehet a dolgozat megértéséhez. Az első általunk ismertetett eszköz a matroidok Tutte-polinomja. A 2. fejezetben megmutatjuk, hogy milyen szoros a kapcsolat egy lineáris kód és az általa meghatározott mátrix-matroid között (a matroidelméleti alapfogalmakat lásd: 1.2. alfejezetben). Ez érdekes kérdéseket vet fel:
1. A kódok mely paraméterei határozhatóak meg a hozzájuk tartozó mátrix-matroid tulajdonságaiból?
2. Vannak-e olyan kódtulajdonságok, amik egész biztosan nem következnek ezen matroid sajátságaiból?
3. Melyek a matroidok azon tulajdonságai, amikből következtetni tudunk a kódok jellemzőire?
Jó néhány kutatás foglalkozik ezzel a kérdéskörrel napjainkban is, közülük talán az egyik legkiemelkedőbb aktuális eredmény Thomas Britz nevéhez kötődik, aki Henry Crapo és Gian-Carlo Rota híres "Kritikus Tételének" (Critical Theorem) [14] általánosításaiból felállított egy sejtést, miszerint lineáris kódoknak mindazon jellemzője, amely meghatározható a hozzájuk tartozó mátrix-matroidból, megadható két – szintén általa ismertetett – tétel segítségével [7]. Ebben a dolgozatban a Kritikus Tételnek egyedül az a Greene által igazolt következménye szerepel, ami a lineáris kódok súly-számlálóját határozza meg [17], bár a Kritikus Tétellel való kapcsolatra ennél sem fogunk kitérni, sokkal inkább az elért konkrét eredményekre koncentrálunk. A Tutte-polinomból lineáris kódok számos tulajdonsága meghatározható, úgymint a kódszavak hossza, a kód dimenziója, minimális távolsága vagy akár a súly-számláló. Ezekbe enged betekintést a 3.2. alfejezet és ezek alapján fogalmazódott meg a kérdés Peter Cameronban 2001-ben [11], hogy vajon megállapítható-e a térlefedő kódok elérési sugara is a Tutte-polinomból. A negatív választ Thomas Britz és Carrie G. Rutherford adta meg 2005-ben [6] két olyan generátormátrixszal, melyekhez tartozó mátrix-matroidok Tutte-polinomja azonos, az általuk generált kódok elérési sugara viszont eltér. Skorobogatov munkássága [38] alapján Britz és Rutherford azt is megmutatta, hogy lineáris kódok elérési sugara a hozzájuk tartozó matroidok semilyen tulajdonságából nem következtethető ki általános esetben [6]. Ezeket az ellenpéldákat a 3.3. alfejezetben ismertetjük.

A 4. fejezetben az úgynevezett gráfelméleti kódokat vizsgáljuk. Mutatunk példát arra, hogy a gráfelméleti vágás-kód esetében a WDCL (weight distribution of coset leaders) a Tutte-polinom és az elérési sugár együttes ismeretéből sem állapítható meg. Meglepő eredmény a gráfelméleti kódok kapcsán, hogy míg a minimális távolság pusztán egyszerű matroidelméleti tételekkel

meghatározható, addig az elérési sugár még a súly-számláló ismeretében sem egyértelmű. Ennek ellenére az elérési sugár expliciten meghatározható egyéb kombinatorikai eszközökkel, nevezetesen a gráfelméleti átfogalmazás segítségével.

Az 5. fejezetben bizonyos fajta bináris szürjektív kódok dimenziószámának keressük a maximális lehetséges értékét rögzített kódméret mellett. A szürjektív és általánosított szürjektív kódok széles körben alkalmazhatóak, ám egyelőre kevés pontos érték van meghatározva a kérdéskörben. A kód mátrix alakjának duális megfordítása egy speciális tulajdonságú extremális halmazrendszert eredményez. Mi ebből a nézőpontból közelítettük meg a kérdést, ez a következő kombinatorikai eszköz, amit kódelméleti problémák megoldásához használhatunk. A 2-szürjektív kódok az úgynevezett kvalitatív független halmazrendszereknek felelnek meg, míg a speciálisabb $m-2$ hiányú m-szürjektív kódok azokkal a halmazrendszerekkel ekvivalensek, melyekre tejesül, hogy bármely m elemük között van két kvalitatív független, tehát láthatjuk, hogy szoros a kapcsolat a két terület között. Egy kódot akkor nevezünk m-szürjektívnek, ha bármely m helyen bárhogy meghatározva a komponensek értékét, van legalább egy kódszó, ami illeszkedik az előírt m komponensre. Két halmaz kvalitatív függetlensége pedig azt jelenti, hogy négy nem-üres részre bontják az alaphalmazt, vagyis $A \cap B$, $\overline{A} \cap B$, $A \cap \overline{B}$, $\overline{A} \cap \overline{B}$ semelyike nem üres. (A kvalitatív független halmazrendszerek nem csupán eszközök a kódelméleti kérdések megválaszolásában, önmagukban is vizsgálatok tárgyai kereséselméleti vonatkozásuk miatt.) m-kvalitatív független halmazrendszerek – vagyis azok, melyeknek bármely m eleme között van két kvalitatív független – elemszámára páratlan m esetén sikerült éles felső becslést adni, páros m esetén pedig egy sejtést felállítani éles korlátról. A szakdolgozat témáját ez az eredmény motiválta, ennek köszönhetően fogalmazódott meg bennem a kérdés, hogy a mesterképzés alatt megismert kombinatorikus struktúrák vajon nem alkalmazhatóak-e szintén kódelméleti problémák megválaszolására. Ezen alkalmazásokból adunk most ízelítőt.

1.1. Kódelméleti alapismeretek

Ebben az alfejezetben közöljük mindazon kódelméleti definíciót és állítást, melyeket használni fogunk a dolgozatban. A kimondott állítások mindegyike könnyen meggondolható, de [20]-ban, illetve [29]-ben megtalálhatóak a bizonyítások, sok egyéb hasznos kódelméleti ténnyel együtt.

A továbbiakban legyen q prímhatvány, és jelölje $\mathbb{F}_q$ a q elemű véges testet.

Definíció. Az $x, y \in \mathbb{F}_q^n$ pontok *Hamming-távolsága* alatt azon koordináták számát értjük, melyek az adott két szóban különböznek egymástól. Jelölés: $d(x, y)$.

Definíció. *Hamming-térnek* nevezzük a Hamming-távolsággal, mint metrikával ellátott $\mathbb{F}_q^n$ vektorteret.

Definíció. A Hamming-tér egy tetszőleges nem üres részhalmazát *kódnak*, e halmaz elemeit pedig *kódszavaknak* nevezzük.

A dolgozatban előkerülő kódoknak két alapvető tulajdonságát vizsgáljuk:

1. *Térlefedő tulajdonságról* beszélünk, ha azt a legkisebb R értéket keressük, melyre teljesül, hogy az $\mathbb{F}_q^n$ Hamming-tér minden eleme legfeljebb R Hamming-távolságra van valamely kódszótól.
Az R paraméter neve *elérési sugár* (covering radius), értéke a Hamming-távolsággal kifejezve:

$$R = \max_{y \in \mathbb{F}_q^n} \min_{x \text{ kódszó}} d(x, y).$$

2. *Hibajavító tulajdonságról* beszélünk, ha azt a legnagyobb d értéket keressük, melyre teljesül, hogy bármely két kódszó Hamming-távolsága legalább d.
A d paraméter neve *minimális távolság*, értéke a Hamming-távolsággal kifejezve:

$$d = \min\{d(x, y) : \ x, y \text{ kódszó}, \ x \neq y\}.$$

A hibajavító elnevezés abból ered, hogy a C kód hibajavítóképessége kifejezhető a minimális távolsággal:

Definíció. Egy C kód t-hibajavító, ha tetszőleges üzenetben előforduló legfeljebb t számú hibát ki tud javítani, azaz ha két különböző kódszó mindegyikének értékét legfeljebb t helyen megváltoztatva (ezek a helyek a két kódszó esetében lehetnek különbözőek) nem kaphatjuk a Hamming-térnek ugyanazt az elemét.

1.1. Állítás. *Egy C kód pontosan akkor t-hibajavító, ha $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$.*

Definíció. A C kódot q,n,k paraméterű *lineáris kódnak* nevezzük, ha C az $\mathbb{F}_q^n$ Hamming-tér k dimenziós altere. Jelölés: $C(n, k; q)$.

Definíció. A $C(n, k; q)$ lineáris kód *generátormátrixa* egy olyan $A \in \mathbb{F}_q^{k \times n}$ mátrix, melynek sorai C bázisát alkotják.

1.2. Megjegyzés. *Az A és A' generátormátrixok pontosan akkor tartoznak ugyanahhoz a $C(n, k; q)$ kódhoz, ha $A' = BA$, ahol $B \in \mathbb{F}_q^{k \times k}$ nemszinguláris mátrix (egy bázistranszformáció mátrixa).*

Definíció. A $C(n, k; q)$ és a $C'(n, k; q)$ kódot *ekvivalensnek* nevezzük, ha a C-beli kódszavak egy $P \in \mathbb{F}_q^{n \times n}$ monomiális mátrixszal való szorzással (aminek minden sorában és oszlopában pontosan egy nem nulla elem van) átvihetők C' kódszavaiba.
Tehát ekvivalens kódokat eredményező transzformáció a koordináták felcserélése, illetve $\mathbb{F}_q^*$-beli elemekkel szorzása.

Ez alapján az $A \in \mathbb{F}_q^{k\times n}$ és az $A' \in \mathbb{F}_q^{k\times n}$ mátrix pontosan akkor generál ekvivalens kódokat, ha $A' = BAP$, ahol $B \in \mathbb{F}_q^{k\times k}$ egy bázistranszformáció mátrixa, $P \in \mathbb{F}_q^{n\times n}$ pedig monomiális.

Definíció. A $C(n,k;q)$ lineáris kód *paritásellenőrző mátrixa* egy olyan $H \in \mathbb{F}_q^{n-k\times n}$ mátrix, melyre teljesül, hogy $C = \ker(H^T)$, azaz $x \in C \Leftrightarrow xH^T = 0$.

1.3. Állítás. *Egy C lineáris kód minimális távolsága pontosan akkor d, ha a C paritásellenőrző mátrixának oszlopai közül bármely $d-1$ lineárisan független, de kiválasztható d oszlopvektor úgy, hogy azok már lineárisan összefüggőek.*

Definíció. A $C(n,k;q)$ kód *duális kódja* az ($\mathbb{F}_q^n$-beli) ortogonális kiegészítő altere. Jelölés: $C^\perp$.
Tehát

$$C^\perp = \{y \in \mathbb{F}_q^n : \ x \cdot y = 0, \ \forall x \in C\},$$

ahol $x \cdot y$ jelöli x és y skalárszorzatát.

1.4. Állítás. *Legyen C lineáris kód. Ekkor*
(i) ha C q,n,k paraméterű, akkor a $C^\perp$ kód $q,n,n-k$ paraméterű,
(ii) $(C^\perp)^\perp = C$,
(iii) H pontosan akkor paritásellenőrző mátrixa a C kódnak, ha H^T generátormátrixa $C^\perp$-nak.

Definíció. Egy $c \in \mathbb{F}_q^n$ kódszó *súlya* a nem nulla koordinátáinak száma. Jelölés: $w(c)$.

Definíció. Egy C lineáris kód *súly-számlálója* (weight-enumerator) alatt a következő polinomot értjük:

$$W_C(x,y) = \sum_{c\in C} x^{n-w(c)}y^{w(c)} = \sum_{i=0}^{n} A_i x^{n-i}y^i,$$

ahol A_i az i súlyú kódszavak száma.
Ezt egyváltozós polinomként is szokták értelmezni, mert az x helyére 1-et helyettesítve nem veszítünk információt:

$$W_C(z) = \sum_{c\in C} z^{w(c)} = \sum_{i=0}^{n} A_i z^i,$$

de mi most az általánosabb, kétváltozós alakkal fogunk dolgozni.

Legyen $C = \{\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_s\} \subseteq \mathbb{F}_q^n$ egy q,n,k paraméterű lineáris kód. Világos, hogy ekkor $s = q^k$ és $\exists i : \mathbf{c}_i = \mathbf{0}\,(1 \le i \le s)$. Vegyünk egy tetszőleges $\mathbf{v}_1 \in \mathbb{F}_q^n \setminus C$ vektort, és képezzük az alábbi halmazt: $C + \{\mathbf{v}_1\} = \{\mathbf{c}_1 + \mathbf{v}_1, \mathbf{c}_2 + \mathbf{v}_1, ..., \mathbf{c}_s + \mathbf{v}_1\}$. Ezután válasszunk egy $\mathbf{v}_2 \in \mathbb{F}_q^n \setminus (C \cup (C + \{\mathbf{v}_1\}))$ vektort, és képezzük a következő halmazt: $C + \{\mathbf{v}_2\} = \{\mathbf{c}_1 + \mathbf{v}_2, \mathbf{c}_2 + \mathbf{v}_2, ..., \mathbf{c}_s + \mathbf{v}_2\}$. Ezt az eljárást

addig folytatjuk (mindig egy tetszőleges $\mathbf{v}_j \in \mathbb{F}_q \setminus (C \cup \bigcup_{i=1}^{j-1} (C + \{\mathbf{v}_i\}))$ vektort véve és azzal a $C + \{\mathbf{v}_j\}$ halmazt képezve), amíg $\mathbb{F}_q^n$ minden eleme bele nem kerül valamelyik halmazba.

1.5. Állítás. *Az imént definiált halmazok $\mathbb{F}_q^n$ egy partícióját alkotják.*

Definíció. Az így előálló $C + \{\mathbf{0}\}, C + \{\mathbf{v}_1\}, ..., C + \{\mathbf{v}_r\}$ halmazokat *C-szerinti mellékosztályoknak* (coset), a $\{\mathbf{0}, \mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_r\}$ vektorrendszert pedig a mellékosztályok egy *reprezentánsrendszerének* nevezzük.

A mellékosztályok összetétele nem függ a reprezentánsok választásától, ezért megtehetjük, hogy olyan reprezentánsrendszert választunk, amelyben minden vektor a saját mellékosztályának egy minimális súlyú eleme. Ezeket a minimális súlyú elemeket *osztályelsőnek* (coset leader) nevezzük.

Az osztályelsőknek tekinthetjük az úgynevezett *súly-eloszlását*, ami egy olyan számsorozat, melynek i-edik tagja azt mutatja, hogy az osztályelsők között hány i súlyú található. Ennek a számsorozatnak az első tagja mindig 1 lesz, hiszen a $C + \{\mathbf{0}\}$ mellékosztály legkisebb súlyú eleme az azonosan nulla kódszó, és ez más mellékosztályban nem szerepelhet. Az osztályelsőknek ezt a súly-eloszlását röviden WDCL-nek fogjuk hívni az angol weight distribution of coset leaders elnevezés miatt.

1.6. Megjegyzés. *Egy lineáris kód elérési sugara eggyel kisebb, mint a WDCL elemszáma, tehát*

$$R(C) = \max\{w(c) : c \in C \text{ osztályelső}\}.$$

1.2. Felhasznált matroidelméleti alapismeretek

Ebben a matroidelméleti bevezetőben csupán azok az ismeretek szerepelnek, amiket a későbbiekben fel fogunk használni. A matroidokról alapos áttekintést [16]-ben, [43]-ben és [33]-ben találhat az olvasó.

Definíció. Egy $M = (E, \mathcal{F})$ pár *matroid*, ha E véges halmaz és $\mathcal{F}$ az E részhalmazainak olyan halmaza, amely teljesíti az alábbi tulajdonságokat:
(F1) $\varnothing \in \mathcal{F}$,
(F2) ha $F \in \mathcal{F}$, akkor $\forall F' \subseteq F : F' \in \mathcal{F}$,
(F3) ha $F_1, F_2 \in \mathcal{F}$ és $|F_1| < |F_2|$, akkor $\exists e \in F_2 \setminus F_1 : F_1 \cup \{e\} \in \mathcal{F}$.

Az E véges halmazt a matroid *alaphalmazának*, $\mathcal{F}$ elemeit a matroid *függetlenjeinek*, a nem független halmazokat pedig *függőnek* nevezzük.

Definíció. Két matroid *izomorf*, ha létezik az alaphalmazaik között olyan bijekció, amelynél pontosan a független halmazok képe lesz független.

Az alaphalmaz maximális független részhalmazai a bázisok, minimális függő részhalmazai pedig a körök. Formálisan:

Definíció. Az $M = (E, \mathcal{F})$ matroid alaphalmazának egy B részhalmaza *bázis*, ha $B \in \mathcal{F}$, de $\forall B' \supset B : B' \notin \mathcal{F}$.
A bázisok halmazát jelöljük $\mathcal{B}$-vel.

Definíció. Az $M = (E, \mathcal{F})$ matroid alaphalmazának egy C részhalmaza *kör*, ha $C \notin \mathcal{F}$, de $\forall C' \subset C : C' \in \mathcal{F}$.
A körök halmazát jelöljük $\mathcal{C}$-vel.

A matroid definiálására használatban vannak az itt felírt $(F1), (F2), (F3)$ axiómarendszerrel ekvivalens más függetlenségi axiómarendszerek, például az $(F3)$ axióma egy ekvivalens átfogalmazása a következő:
(F3') minden $X \subseteq E$ halmazra az X-ben fekvő maximális függetlenek ugyanakkora elemszámúak.
Ezt az elemszámot X *rangjának* nevezzük és $r(X)$-szel jelöljük.
Egy $M = (E, \mathcal{F})$ matroid rangján az alaphalmazának rangját, vagyis a bázisainak elemszámát értjük: $r(M) = r(E) = |B|$, ahol B bázis M-ben.

Definíció. Az M matroid *generátorai* az alaphalmaz azon X részhalmazai, melyekre $r(X) = r(M)$ teljesül, vagyis azok a részhalmazok, amik tartalmaznak bázist.

Nem véletlen, hogy többféle függetlenségi axiómarendszerrel is szokás definiálni a matroidot. A gyengébb axiómarendszerek olyankor hasznosak, amikor egy konkrét stuktúráról szeretnénk megmutatni, hogy matroid, az erősebbek pedig olyankor, amikor általánosan matroidokról kell valamit belátnunk.

De nem csupán az $\mathcal{F}$ halmazrendszerre tett kikötésekkel kaphatunk matroidot:
A bázisok halmaza egyértelműen meghatározza a függetleneket:
$\mathcal{F} = \{F \subseteq E : \exists B \in \mathcal{B} : F \subseteq B\}$, ha tehát sikerül megfogalmaznunk olyan tulajdonságokat, hogy azokat feltéve $\mathcal{B}$-re épp egy matroid bázisait kapjuk, akkor ennek a bázis-axiómarendszernek a segítségével is definiálható a matroid.

1.7. Állítás. *Legyen E véges halmaz. A $\mathcal{B} \subseteq \mathcal{P}(E)$ halmazrendszer akkor csak akkor alkotja egy matroid bázisainak halmazát, ha teljesíti az alábbi tulajdonságokat:*
(B1) *$\mathcal{B} \neq \emptyset$,*
(B2) *ha $B_1, B_2 \in \mathcal{B}$ és $x_1 \in B_1 \setminus B_2$, akkor létezik $x_2 \in B_2 \setminus B_1$, úgy hogy $B_1 \setminus \{x_1\} \cup \{x_2\} \in \mathcal{B}$.*

Bizonyítás. Azt kell megmutatnunk, hogy az $\mathcal{F} = \{F : \exists B \in \mathcal{B} : F \subseteq B\}$ halmazrendszer teljesíti a függetlenségi axiómákat és hogy egy matroid bázisaira teljesül a fenti két tulajdonság.

A $(B1)$ axióma szerint $\mathcal{B}$ nem üres: $\exists B \in \mathcal{B}$. Az üreshalmaz minden halmaznak – így B-nek is – részhalmaza, amiből $\mathcal{F}$ definíciója alapján következik, hogy $\varnothing \in \mathcal{F}$, ami épp az $(F1)$ axióma. $(F2)$ fennállása is triviálisan következik $\mathcal{F}$ definíciójából. $(F3)$ bizonyításához szükségünk lesz $(B2)$-nek arra az egyszerű következményére, hogy minden $\mathcal{B}$-beli halmaznak ugyanannyi az elemszáma. Vegyünk olyan $F_1, F_2 \in \mathcal{F}$ halmazokat, melyekre $|F_1| < |F_2|$. Legyen B_1 az F_1-et, B_2 az F_2-t tartalmazó $\mathcal{B}$-beli halmaz. Ha $B_1 \cap (F_2 \setminus F_1) \neq \varnothing$ és $e \in B_1 \cap (F_2 \setminus F_1)$, akkor $F_1 \cup \{e\} \in \mathcal{F}$, vagyis $(F3)$ teljesül. Tehát feltehető, hogy $B_1 \cap (F_2 \setminus F_1) = \varnothing$ és alkalmazzuk $(B2)$-t $B_1 \setminus (F_1 \cup B_2)$ minden elemére. Mivel $|F_1| < |F_2|$ és $|B_1| = |B_2|$, ezért lesz olyan $B_1 \setminus F_1$-beli elem, amit egy F_2-beli e' elemre cserélünk ki, így $F_1 \cup \{e'\}$ része egy $\mathcal{B}$-belinek, vagyis $F_1 \cup \{e'\} \in \mathcal{F}$. Ezzel megmutattuk, hogy $\mathcal{F}$ valóban egy matroid független halmazaiból áll.
$(F3')$ miatt *minden bázis azonos elemszámú*, amiből $(F2)$ felhasználásával következik a $(B2)$ tulajdonság (hiszen $|B_1 \setminus \{x_1\}| < |B_2|$), $(F1)$-ből pedig adódik $(B1)$, így az állítás mindkét irányát beláttuk. □

1.8. Megjegyzés. *A független halmazok meghatározhatóak pusztán a rangfüggvény vagy a körök halmazának ismeretében is:* $\mathcal{F} = \{F \subseteq E : r(F) = |F|\} = \{F \subseteq E : \nexists C \in \mathcal{C} : C \subseteq F\}$*, és könnyen megadhatók a megfelelő axiómák, amiket teljesítve az* (E, r) *illetve* $(E, \mathcal{C})$ *pár matroid, de nekünk ezen axiómák ismeretére a dolgozat megértéséhez nincs szükségünk.*

A bázisokra fennálló $(B2)$ *kicserélési tulajdonságból* bebizonyítható az úgynevezett *becserélési tulajdonság*:

1.9. Állítás. *Ha* $B_1, B_2 \in \mathcal{B}$ *és* $x_2 \in B_2 \setminus B_1$*, akkor létezik* $x_1 \in B_1 \setminus B_2$*, úgy hogy* $B_1 \setminus \{x_1\} \cup \{x_2\} \in \mathcal{B}$*.*

Bizonyítás. Használjunk $k = |B_1 \setminus B_2| = |B_2 \setminus B_1|$ szerinti teljes indukciót! A $k = 0$ esetben az állítás semmitmondó, $k = 1$-re pedig triviálisan teljesül. Tegyük fel, hogy $k \geq 2$ és az egymást k-nál kevesebb elemben metsző bázispárokra igaz az állítás. Vegyünk egy $x_2 \neq x_2' \in B_2 \setminus B_1$ elemet (ilyen létezik, mivel $k \geq 2$). Ekkor $(B2)$ szerint $\exists x_1' \in B_1 \setminus B_2 : B_2' = B_2 \setminus \{x_2'\} \cup \{x_1'\} \in \mathcal{B}$. Mivel $|B_1 \setminus B_2'| = k - 1$, az indukciós feltevést használva $\exists x_1 \in B_1 \setminus B_2'$: $B_1 \setminus \{x_1\} \cup \{x_2\} \in \mathcal{B}$. □

Az M matroid *duálisa* alatt azt a matroidot értjük, melynek alaphalmaza megegyezik M alaphalmazával és a bázisai pontosan M bázisainak komplementerei. Az M matroid duálisát M^*-gal, bázisainak halmazát $\mathcal{B}^*$-gal jelöljük. Lássuk be, hogy M^* valóban matroid!

1.10. Állítás. $\mathcal{B}^*$ *kielégíti a bázisaxiómákat.*

Bizonyítás. Mivel M matroid, világos, hogy $(B1)$ teljesül. A $(B2)$ axióma M^*-ra így hangzik: ha $B_1^*, B_2^* \in \mathcal{B}^*$ és $x_1 \in B_1^* \setminus B_2^*$, akkor létezik $x_2 \in B_2^* \setminus B_1^*$, úgy hogy $B_1^* \setminus \{x_1\} \cup \{x_2\} \in \mathcal{B}^*$. Legyen $B^* = E \setminus B_1$, $B_2^* = E \setminus B_2$, ahol $B_1, B_2 \in \mathcal{B}$. $(B2)$ igazolásához tehát azt kell megmutatnunk, hogy $\forall x_1 \in B_2 \setminus B_1 : \exists x_2 \in B_1 \setminus B_2 : B_1 \setminus \{x_2\} \cup \{x_1\} \in \mathcal{B}$, ami épp a becserélési tulajdonság, így $M^* = (E, \mathcal{B}^*)$ tényleg matroid. □

1.11. Állítás. *Legyen r az $M = (E, \mathcal{B})$ matroid rangfüggvénye, r^* pedig a duális $M^* = (E, \mathcal{B}^*)$ matroid rangfüggvénye. Ekkor minden $X \subseteq E$ halmazra:*

$$r^*(X) = |X| + r(E \setminus X) - r(M).$$

Bizonyítás. Az X halmaz M^*-beli rangja azt mondja meg, hogy legfeljebb hány elemmel metszhetnek bele X-be a $\mathcal{B}^*$-beli B^* bázisok. Felhasználva, hogy $\forall B \in \mathcal{B} : |B| = r(E)$, a következő egyenlőséglánccal bizonyítható az állítás:

$$r^*(X) = \max |X \cap B^*| = |X| - \min |X \cap B| = |X| - (|B| - \max |B \setminus X|) =$$

$$= |X| - (r(M) - r(E \setminus X)) = |X| + r(E \setminus X) - r(M).$$

□

1.12. Következmény. *Ha $X \subseteq E$ és $X^* = E \setminus X$, akkor az r^*-ra felírt formulából rögtön következik az alábbi két egyenlőség, ami a következő fejezetben hasznos lesz számunkra:*

$$r^*(M^*) - r^*(X^*) = |X| - r(X), \quad |X^*| - r^*(X^*) = r(M) - r(X).$$

Az egy elemű kört *huroknak*, az olyan elemet, ami minden bázisban benne van *hídnak* nevezzük.

Definíció. Ha $e \in E$ nem hurokelem és $\mathcal{F}' = \{F \subseteq E \setminus \{e\} : F \cup \{e\} \in \mathcal{F}\}$, akkor az $M/e = (E \setminus \{e\}, \mathcal{F}')$ az $M = (E, \mathcal{F})$ matroid *összehúzottja* $E \setminus \{e\}$-re.

(Itt azt, hogy e nem hurokelem, azért kell feltennünk, hogy M/e matroid legyen, hiszen ha e hurokelem lenne, akkor $\varnothing \in \mathcal{F}'$ nem teljesülne.)

Definíció. Ha $e \in E$ nem híd és $\mathcal{F}'' = \{F \subseteq E \setminus \{e\} : F \in \mathcal{F}\}$, akkor az $M\backslash e = (E \setminus \{e\}, \mathcal{F}'')$ az $M = (E, \mathcal{F})$ matroid *megszorítása* $E \setminus \{e\}$-re.

A definíciókból világos, hogy M/e és $M\backslash e$ is matroid.

Jelölés: Jelölje r' az M/e matroid, r'' pedig az $M\backslash e$ matroid rangfüggvényét.

Most mutatunk néhány olyan példát matroidra, melyeknek a későbbiekben fontos szerepe lesz. Elsőként vizsgáljuk a mátrixokból kapott matroidokat!
A továbbiakban legyen $\mathbb{F}$ tetszőleges test.

1.13. Állítás. *Legyenek $a_1, a_2, ..., a_n$ egy tetszőleges $A \in \mathbb{F}^{m\times n}$ mátrix oszlopvektorai, $E := \{1, 2, ..., n\}$ és $\mathcal{F}$ álljon azokból az $F \subseteq E$ halmazokból, melyekre $\{a_i : i \in F\}$ lineárisan független vektorrendszer. Ekkor az $M[A] := (E, \mathcal{F})$ pár egy matroid.*

Bizonyítás. $(F1)$, $(F2)$ triviálisan teljesül, $(F3)$ pedig a lineáris algebra egy elemi tétele. □

Definíció. Az így kapott $M[A]$-t *lineáris* vagy *mátrix-matroidnak* nevezzük, $\mathbb{F} = \mathbb{F}_2$ esetén pedig *bináris matroidokról* beszélünk.

Ha egy M matroid izomorf valamely $\mathbb{F}$ test feletti A mátrix $M[A]$ mátrix-matroidjával, akkor azt mondjuk, hogy M *reprezentálható* $\mathbb{F}$ *felett* (röviden: $\mathbb{F}$*-reprezentálható*) és A az M egy $\mathbb{F}$ feletti *reprezentációja.*

1.14. Megjegyzés. *Ha A'-t A-ból elemi sorekvivalens átalakításokkal kapjuk (két sor felcserélése; valamely sor elemeinek egy $\mathbb{F}^*$-beli számmal történő végigszorzása; valamely sornak egy másik sorhoz való hozzáadása; csupa* 0*-sor elhagyása (ha nem ez az egyetlen sor)), akkor $M[A'] = M[A]$; A' és A ugyanannak a matroidnak két $\mathbb{F}$-reprezentációja. Tehát mindig feltehető, hogy egy mátrix-matroid olyan mátrixhoz tartozik, melynek sorai lineárisan függetlenek.*

1.15. Állítás. $\mathbb{F}$*-reprezentálható matroid duálisa is* $\mathbb{F}$*-reprezentálható.*

Bizonyítás. A bizonyítás lényege, hogy M egy reprezentáló mátrixából megkonstruálható M^* egy reprezentáló mátrixa. ([33], 2.2. fejezet) □

A második példánkban a független halmazok az elemszámuk korlátozásával lesznek meghatározva:

Definíció. Ha $|E| = n$, $k \in \mathbb{Z}$, $0 \le k \le n$ és $\mathcal{F} = \{X \subseteq E : |X| \le k\}$, akkor az $(E, \mathcal{F})$ párt *uniform matroidnak* nevezzük és $U_{n,k}$-val jelöljük.

Könnyen ellenőrizhető, hogy az így definiált $\mathcal{F}$ halmazra mindhárom függetlenségi axióma teljesül, így $U_{n,k}$ valóban matroid.

Végül egy másik fontos – és általunk használt – példája a matroidoknak:

Definíció. Ha az E alaphalmaz egy G irányítatlan gráf élhalmaza és $\mathcal{F}$ azokból az $F \subseteq E$ halmazokból áll, melyek nem tartalmaznak kört, akkor az $(E, \mathcal{F})$ párt *körmatroidnak* nevezzük és $M[G]$-vel jelöljük.

Ha egy M matroid izomorf valamely G gráf $M[G]$ körmatroidjával, akkor M-et *grafikus matroidnak* nevezzük.

A bemutatott definíciókat/műveleteket mindenképp érdemes végiggondolni legalább a körmatroid esetén, mert ez legtöbbször szemléletesen segít megérteni az általános esetet.

Kimondunk két egyszerű, körmatroidra vonatkozó tételt, melyeket a gráfelméleti kódokról szóló 4. fejezetben fogunk alkalmazni.

1.16. Tétel. *Ha E egy G gráf élhalmaza, $\mathcal{C}$ pedig a G-beli körök élhalmazainak halmaza, azaz $\mathcal{C} = \{E(C) : C \text{ kör } G\text{-ben}\}$, akkor $\mathcal{C}$ épp az $M[G]$ matroid köreiből áll.*

Ennek a tételnek a bizonyításához szükséges lenne a kör-axiómák megfogalmazása. A bizonyítást lásd: [33], 11. oldal, Proposition 1.1.7.

1.17. Tétel. *Irányítatlan gráf körmatroidja minden test felett reprezentálható.*

A bizonyítást lásd: [16] 1.2.6. Tétel.

2. Kódok és mátrix-matroidok kapcsolata

Definíció. Legyen az A mátrix a $C(n,k;q)$ lineáris kód generátormátrixa. Ekkor az $M[A]$ (k rangú) mátrix-matroidot a C *kódon vett matroidnak* nevezzük, és M_C-vel jelöljük.

2.1. Megjegyzés. *M_C nem függ a generátormátrix választásától, csak a kódtól.*

2.2. Megjegyzés. *Ha a C és C' lineáris kódok ekvivalensek, akkor a rajtuk vett M_C és $M_{C'}$ matroidok izomorfak.*

Definíció. Legyen az $A \in \mathbb{F}_q^{k\times n}$ mátrix az M matroid egy olyan $\mathbb{F}_q$-reprezentációja, melynek sorvektorai lineárisan függetlenek $\mathbb{F}_q^n$-ben. Ekkor azt a $C(n,k;q)$ lineáris kódot, melynek generátormátrixa A, az *M matroidból A szerint nyert kódnak* nevezzük, és $C_M(A)$-val jelöljük.

A 3.2. alfejezetben szükségünk lesz rá, hogy összehúzott, illetve megszorított matroidokból nyert kódokkal dolgozzunk, ezért gondoljuk meg, hogy milyen hatással van az $M = (E, \mathcal{F})$ matroid $E \setminus \{e_i\}$-re vett összehúzása (ha $e_i \in E$ nem hurok) és megszorítása (ha $e_i \in E$ nem híd) a belőle nyert kódokra!

Definíció. Ha a C kódnak létezik olyan A generátormátrixa, melynek i-edik oszlopában az első elem 1, a többi pedig 0, akkor definiáljuk a *C' i-vel rövidített kódot* (shortened code) úgy, mint az által az A' mátrix által generált lineáris kód, melyet úgy kapunk, hogy elhagyjuk A első sorát és i-edik oszlopát.

Definíció. Vegyük a C kódnak egy olyan A generátormátrixát, melynek i-edik oszlopában legfeljebb az első elem nem nulla. Ha A nem hozható elemi sorekvivalens átalakításokkal olyan alakúra, hogy az i-edik oszlopban továbbra is legfeljebb az első elem nem nulla és az első sorban csak az i-edik elem nem nulla, akkor legyen a *C" i-ben lyukasztott kód* (punctured code) az által az A" mátrix által generált, melyet úgy kapunk, hogy elhagyjuk A-ból az i-edik oszlopot.

2.3. Állítás. *Legyen M egy k rangú $\mathbb{F}_q$-reprezentálható matroid az n elemű E alaphalmazon és legyen $A \in \mathbb{F}_q^{k\times n}$ az M egy olyan reprezentáló mátrixa, melyben az i-edik oszlopnak legfeljebb az első eleme nem nulla. Ekkor*

$$C' = C_{M/e_i}(A) \text{ és } C" = C_{M\setminus e_i}(A).$$

Bizonyítás. A bizonyításhoz elég visszaemlékeznünk a megszorítás és az összehúzás definíciójára, valamint megvizsgálni, hogy a generátormátrixok nyelvén mit is jelent az, hogy E egy eleme hurok, illetve híd M-ben. (Könnyen meggondolható, hogy az M matroidban egy $e_i \in E$ elem pontosan akkor hurok, ha a reprezentáló mátrixában az e_i elemhez tartozó oszlop lineárisan összefüggő

vektorrendszert alkot $\mathbb{F}_q^k$-ban, vagyis ha az i-edik oszlop minden eleme 0, és pontosan akkor híd, ha az A mátrix elemi sorekvivalens átalakításokkal olyan alakúra hozható, hogy az i-edik oszlopban csak az első elem nem nulla és az első sor i-ediken kívüli elemei is mind nullák.) □

Az alábbi állítás – melyet szintén a 3.2. alfejezetben fogunk használni – megfogalmazza egy lineáris kódhoz- és a duális kódjához tartozó matroid közötti szoros kapcsolatot. A bizonyítása könnyen meggondolható, itt nem részletezzük (lásd: [9] 11. oldal).

2.4. Állítás.

$$(M_C)^* = M_{C^\perp} \tag{1}$$

A következő tétel adódik az előző alfejezetbeli az 1.3. Állításból.

2.5. Tétel. *Legyen H a $C(n,k;q)$ kód paritásellenőrző mátrixa és jelölje d a C kód minimális távolságát. Ekkor fennáll a $d = |\mathfrak{C}|$ egyenlőség, ahol $\mathfrak{C}$ az $M[H]$ matroid legkisebb elemszámú köre.*

Azt nem várhatjuk, hogy egy M_C matroid ismeretében akár ekvivalencia erejéig egyértelműen meghatározzuk az őt megadó kódot (hiszen nem ekvivalens kódokhoz is tartozhatnak izomorf matroidok), de amint azt látni fogjuk, így is megállapítható a C kód számos lényeges jellemzője. Sőt, ehhez sok esetben elegendő a matroidnak csak néhány tulajdonságát vizsgálni.

3. Matroidok Tutte-polinomja

A következőkben olyan eszközként szeretnénk tekinteni a matroidokra, melynek segítségével a hozzájuk tartozó kódokról nemtriviális tulajdonságokat bizonyíthatunk. Mivel ekvivalens kódokból nyert matroidok izomorfak, meg kell ragadnunk a matroidoknak egy invariáns tulajdonságát, ami izomorf matroidokra ugyanazt az eredményt adja.

A Tutte-polinom eleget tesz ennek a követelménynek, és a 3.2. alfejezetben látni fogjuk, hogy valóban tudunk belőle következtetni bizonyos gráfparaméterekre.

3.1. A Tutte-polinom alaptulajdonságai

Definíció. Az $M = (E, \mathcal{F})$ matroid Tutte-polinomja alatt az alábbi kétváltozós polinomot értjük

$$T_M(x,y) = \sum_{X \subseteq E} (x-1)^{r(M)-r(X)} (y-1)^{|X|-r(X)}.$$

A Tutte-polinom kiértékelése nem mindig egyszerű feladat, de számos olyan módszer áll rendelkezésünkre, amely megkönnyíti a dolgunkat. A leggyakrabban használt technikák szemléletes példákon bemutatva megtalálhatóak a [31] cikkben.

Mivel (1) szoros és jól megfogalmazható kapcsolatot mutat egy kódon, illetve a duálisán vett matroid között, érdemes azzal kezdenünk, hogy az 1.12. következmény alapján teljesül a következő egyenlőség

$$T_M(x,y) = T_{M^*}(y,x). \tag{2}$$

Ha sem M, sem pedig M^* Tutte-polinomját nem ismerjük még, akkor célravezető az alábbi rekurziót használnunk, amit sokszor egyenesen a Tutte-polinom definíciójaként adnak meg.

Legyen $\oslash$ az *üres matroid*, melynek alaphalmaza az üreshalmaz és így az egyetlen független halmaza is az üreshalmaz: $\oslash = (\varnothing, \{\varnothing\})$. Világos, hogy $T_{\oslash}(x,y) = 1$, mivel $r(\oslash) = r(X) = |X| = 0$ az alaphalmaz minden X részhalmazára. Ha viszont M nem az üres matroid, akkor értelmes a következő állítás, amiből indukcióval bizonyítható, hogy T kétváltozós, egész együtthatós polinom.

3.1. Állítás. *Legyen M matroid az E nemüres véges alaphalmazon.*
a) Ha $e \in E$ se nem hurok, se nem híd, akkor

$$T_M(x,y) = T_{M/e}(x,y) + T_{M\setminus e}(x,y),$$

b) ha $e \in E$ hurokelem, akkor

$$T_M(x,y) = y \cdot T_{M\setminus e}(x,y),$$

c) ha pedig $e \in E$ híd, akkor

$$T_M(x,y) = x \cdot T_{M/e}(x,y).$$

Bizonyítás. Csak az állítás a) részét fogjuk megmutatni, a b) és a c) hasonló megfontolásokból könnyen adódik. Ha r' az M/e, r" pedig az $M\setminus e$ matroid rangfüggvénye, akkor a bizonyítandó azonosság a következő:

$$\sum_{X\subseteq E}(x-1)^{r(M)-r(X)}(y-1)^{|X|-r(X)} =$$

$$= \sum_{X\subseteq E\setminus\{e\}}(x-1)^{r'(M/e)-r'(X)}(y-1)^{|X|-r'(X)} + \sum_{X\subseteq E\setminus\{e\}}(x-1)^{r"(M\setminus e)-r"(X)}(y-1)^{|X|-r"(X)}.$$

A bal oldalt ketté tudjuk bontani aszerint, hogy a kijelölt e elem benne van-e a vizsgált X halmazban. Állapítsuk meg a jobb oldalon szereplő halmazok M/e és $M\setminus e$-beli rangját, és írjuk fel csak az r rangfüggvényt használva az egyenletet!
Egy halmaz pontosan akkor független M/e-ben, ha e-vel kibővítve független M-ben, ezért

$$r'(M/e) = r'(E\setminus\{e\}) = r(E) - 1$$

és tetszőleges $X \subseteq E\setminus\{e\}$ halmazra $r'(X) = r(X\cup\{e\}) - r(\{e\})$. Mivel e nem hurok,

$$r'(X) = r(X\cup\{e\}) - 1.$$

Továbbá $M\setminus e$-ben egy halmaz pontosan akkor független, ha nem tartalmazza e-t és független M-ben. Mivel e-ről feltettük, hogy nem híd, ezért van olyan B bázisa M-nek, hogy $e \notin B$, vagyis $B \in \mathcal{B}$ bázis $M\setminus e$-ben is. Így

$$r"(M\setminus e) = r"(E\setminus\{e\}) = r(E) \text{ és } r"(X) = r(X).$$

Behelyettesítve a következőt kapjuk:

$$\sum_{X\subseteq E\setminus\{e\}}(x-1)^{r(E)-r(X)}(y-1)^{|X|-r(X)} +$$

$$+ \sum_{X\cup\{e\}\subseteq E}(x-1)^{r(E)-r(X\cup\{e\})}(y-1)^{|X\cup\{e\}|-r(X\cup\{e\})} =$$

$$\sum_{X\subseteq E\setminus\{e\}}(x-1)^{(r(E)-1)-(r(X\cup\{e\})-1)}(y-1)^{|X|-(r(X\cup\{e\})-1)} +$$

$$+ \sum_{X\subseteq E\setminus\{e\}}(x-1)^{r(E)-r(X)}(y-1)^{|X|-r(X)},$$

amiről egyszerűsítés és $|X \cup \{e\}| = |X|+1$ felhasználása után már valóban látjuk, hogy azonosság. □

Fontos megjegyeznünk, hogy T jóldefiniált abban az értelemben, hogy a végeredmény nem függ a rekurziós lépésekhez választott elemek sorrendjétől.

A Michael Barany által adott program az $\mathbb{F}$-reprezentálható matroidok Tutte-polinomjának meghatározására ([2]) szintén ezen a rekurzión alapszik. Továbbá használhatjuk a GAP ([37]), a MAGMA ([41]) vagy a Thomas Britz honlapján ([8]) található, többféle nyelven megírt programokat is $\mathbb{F}$-reprezentálható matroid Tutte-polinomjának megadásához.

Most nézzünk egy példát arra, hogyan alkalmazható ez a rekurzió, ha egy gráf, például az n-hosszú kör körmatroidjának Tutte-polinomját szeretnénk felírni:
Egy tetszőleges élet törölve $n-1$ hosszú utat kapunk, aminek Tutte-polinomja x^{n-1}, tetszőleges él összehúzásával pedig eggyel rövidebb körhöz jutunk. Mivel $T_{M[C_2]} = x + y$, így $T_{M[C_n]} = \sum_{i=1}^{n-1} x^i + y$.
Az n-hosszú kör duálisa egy olyan gráf, mely két csúcsból és a köztük menő n párhuzamos élből áll. (2) alapján ennek a Tutte-polinomját is ismerjük: $T_{M[C_n^*]} = \sum_{i=1}^{n-1} y^i + x$.

Egész kis gráfok körmatroidjának Tutte-polinomja kiértékelhető a legtöbb matematikai szoftvercsomaggal (pl.: Maple, Mathematica), és nagyobb gráfok esetén is gyorsan megadható, például a Gary Haggard és David J. Pearce által elérhetővé tett, ingyenesen letölthető programmal ([34]).

Grafikus matroid Tutte-polinomjából számos gráfinvariáns meghatározható, köztük a kromatikus polinom, az erdők száma, feszítőerdők száma. Az utóbbi kettő kiolvasható az alábbi állításból:

3.2. Állítás. *Ha $M = (E, \mathcal{F})$ matroid, akkor*
a) $T_M(0,0) = 0$,
b) $T_M(1,1)$ *a bázisok száma,*
c) $T_M(1,2)$ *a generátorok száma,*
d) $T_M(2,1) = |\mathcal{F}|$ *a független halmazok száma,*
e) $T_M(2,2) = 2^{|E|}$.

Bizonyítás. Az állítás minden része egyenes következménye a definíciónak:

$$T_M(0,0) = \sum_{X \subseteq E} (-1)^{r(M)-r(X)}(-1)^{|X|-r(X)} = \sum_{X \subseteq E} (-1)^{r(M)+|X|} = 0,$$

hiszen E-nek ugyanannyi páros elemű részhalmaza van, mint amennyi páratlan, amiből *a)* következik;
$r(M) = r(X) = |X|$ pontosan akkor teljesül, ha X bázis, amiből *b)* következik;

$r(M) = r(X)$ akkor, ha X tartalmaz bázist, amiből c) következik; $|X| = r(X)$ pedig akkor, ha X független, ami miatt d) és e) is triviálisan teljesül. □

3.2. A Tutte-polinomból meghatározható kódparaméterek

A lineáris C kódon vett M_C matroid Tutte-polinomjának ismeretéből – és így az M_C matroid rang-függvényéből is – számos kódparaméter következik, úgymint a kódhossz, a dimenzió, a minimális távolság vagy épp a súly-számláló. A következő tétel azt mutatja meg, hogy lineáris kódon vett matroid rang-függvénye egyértelműen meghatározza a kód súly-számlálóját.

3.3. Tétel (Greene 1976)**.** *[17] Ha $C(n,k;q)$ lineáris kód, akkor*

$$W_C(x,y) = y^{n-k}(x-y)^k T_{M_C}\left(\frac{x+(q-1)y}{x-y}, \frac{x}{y}\right).$$

Bizonyítás. [9], [10] A tétel bizonyításához szükségünk lesz a Tutte-polinom egy általánosítására. Egy olyan $\widetilde{T}_M(x,y,u,v)$ polinomot keresünk, melyre igaz, hogy

(i) $\widetilde{T}_\varnothing(x,y,u,v) = 1$,
(ii) ha $e \in E$ hurokelem, akkor $\widetilde{T}_M(x,y,u,v) = yu \cdot \widetilde{T}_{M\setminus e}(x,y,u,v)$,
(iii) ha $e \in E$ híd, akkor $\widetilde{T}_M(x,y,u,v) = xv \cdot \widetilde{T}_{M/e}(x,y,u,v)$,
(iv) ha pedig $e \in E$ se nem hurok, se nem híd, akkor

$$\widetilde{T}_M(x,y,u,v) = u \cdot \widetilde{T}_{M\setminus e}(x,y,u,v) + v \cdot \widetilde{T}_{M/e}(x,y,u,v),$$

majd meghatározzuk az x,y,u,v változók értékét úgy, hogy teljesüljön a $W_C = \widetilde{T}_{M_C}(x,y,u,v)$ egyenlőség.

3.4. Lemma. *A Tutte-polinomból az alábbi módon előállított négyváltozós polinom kielégíti a fenti (i) – (iv) feltételeket:*

$$\widetilde{T}_M(x,y,u,v) = u^{|E|-r(M)} v^{r(M)} T_M(x,u).$$

A lemma bizonyítása. Az M/e és $M\setminus e$ matroidok alaphalmaza $E \setminus \{e\}$, amire nyilvánvalóan fennáll, hogy eggyel kisebb elemű, mint az eredeti alaphalmaz. A 3.1. Állítás bizonyítása során megmutattuk, hogy ha $e \in E$ nem hurokelem, akkor

$$r'(M/e) = r(M) - 1,$$

ha pedig $e \in E$ nem híd, akkor

$$r"(M\setminus e) = r(M).$$

Ebből és a 3.1. Állításból egyszerű behelyettesítéssel adódik a lemma. □

3.5. Megjegyzés. *A lemmában mutatott polinom az egyetlen, ami eleget tesz a $\widetilde{T}$-ra megkövetelt feltételeknek.*

Ahhoz, hogy a súly-számlálót azonosítsuk egy $\widetilde{T}$ polinommal, megfogalmazzuk az $(i)-(iv)$ tulajdonságokat kódokra. Legyen a tételben szereplő C lineáris kódnak $A \in \mathbb{F}_q^{k\times n}$ egy generátormátrixa és $M = M_C$. Ekkor A az M_C matroid egy olyan $\mathbb{F}_q$-reprezentációja, hogy $C_{M_C}(A) = C$. A 2. fejezetben láttuk, hogy a matroid összehúzása a kód rövidítésének, a megszorítása pedig a kód lyukasztásának felel meg.

3.6. Lemma. *Legyen C' a C lineáris kód rövidítése az i-edik koordinátával, C" pedig C lyukasztása az i-edik koordinátában. Ekkor a súly-számlálóra az alábbi tulajdonságok teljesülnek:*
(i) $W_{C_\varnothing}(x,y) = 1$.
(ii) Ha az i-edik koordináta hurokelem, akkor $W_C(x,y) = x \cdot W_{C"}(x,y)$.
(iii) Ha az i-edik koordináta híd, akkor $W_C(x,y) = (x+(q-1)y)\cdot W_{C'}(x,y)$.
(iv) Ha az i-edik koordináta se nem hurok, se nem híd, akkor

$$W_C(x,y) = y \cdot W_{C"}(x,y) + (x-y)\cdot W_{C'}(x,y).$$

A lemma bizonyítása. Az üres matroidból nyert kód egyetlen kódszava az azonosan 0 kódszó, emiatt (i) triviálisan teljesül.

Ha az i-edik koordináta hurok, akkor minden kódszó i-edik koordinátája nulla, így az i-edik koordinátában lyukasztott C" kódban $A"_i = A_i$,
$\forall 0 \le i \le n-1$ esetén. C-ben nincs n súlyú kód, hiszen minden kódszóban legalább egy helyen 0 áll és a C"-beli kódszavak hossza 1-gyel rövidebb, mint a C-belieké, ezért $W_C(x,y) = x \cdot W_{C"}(x,y)$ valóban fennáll.

Ha az i-edik koordináta híd, akkor az i-edik koordinátával rövidített C' kód kódszavainak mindegyike q darab C-beli kódszót határoz meg, hiszen az i-edik koordináta helyén $\mathbb{F}_q$ bármely eleme állhat. Ezek közül annak, amelyiknél 0-val bővítettünk, megegyezik a súlya a hozzá tartozó C'-beli kódszó súlyával, a maradék $q-1$ esetben viszont a helyreállított kódszavak súlya eggyel nő, így $W_C(x,y) = (x+(q-1)y)\cdot W_{C'}(x,y)$ is teljesül.

Tegyük most fel, hogy az i-edik koordináta se nem hurok, se nem híd és jelölje C_1 azon C-beli kódszavak halmazát, melyeknek az i-edik komponense 0, W_1 pedig a $\sum_{c\in C_1} x^{n-w(c)}y^{w(c)}$ értéket. Ez alapján vezessük be a C_2 jelölést azon C-beli kódszavak halmazára, melyek i-edik komponense nem nulla, W_2 pedig legyen a $\sum_{c\in C_2} x^{n-w(c)}y^{w(c)}$ érték. A C kód rövidítése után épp a C_1-beli kódszavakat kapjuk, csak egy nulla komponenssel rövidebben, így

$$W_{C'}(x,y) = \frac{W_1}{x},$$

ha pedig kilyukasztjuk a kódot, akkor a C_1-beli és C_2-beli kódszavak eggyel rövidebbek lesznek, a C_1-beliek súlya változatlan marad, a C_2-belieké viszont csökken eggyel, tehát

$$W_{C''}(x,y) = \frac{W_1}{x} + \frac{W_2}{y}.$$

Felhasználva, hogy $W_C(x,y) = W_1 + W_2$ kapjuk, hogy $W_C(x,y) = y \cdot W_{C''}(x,y) + (x-y) \cdot W_{C'}(x,y)$, amivel a lemma (iv) részét is beláttuk. □

A 3.6. Lemmát összevetve a $\widetilde{T}$ polinomra megkövetelt feltételekkel, adódik a következő egyenlőség:

$$W_C(x,y) = \widetilde{T}_{M_C}(x + (q-1)y, x, y, x-y),$$

ebből pedig a 3.4. Lemma alapján kész a tétel bizonyítása:

$$W_C(x,y) = y^{n-k}(x-y)^k T_{M_C}\left(\frac{x+(q-1)y}{x-y}, \frac{x}{y}\right).$$

□

Ennek az eredménynek a segítségével Greene egyszerű bizonyítást adott a MacWilliams-egyenlőségre, ami megmutatja, hogy egy C lineáris kód súly-számlálójából hogyan határozható meg a duális $C^\perp$ kód súly-számlálója.

3.7. Tétel (MacWilliams-egyenlőség)**.** *[30]*

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x + (q-1)y, x-y).$$

Bizonyítás. Alakítsuk át először a bal oldalt, felhasználva, hogy a $C^\perp$ kód $n-k$ dimenziós, $M_{C^\perp} = (M_C)^*$ és $T_M(x,y) = T_{M^*}(y,x)$.

$$W_{C^\perp}(x,y) = y^k(x-y)^{n-k} T_{M_{C^\perp}}\left(\frac{x+(q-1)y}{x-y}, \frac{x}{y}\right) = y^k(x-y)^{n-k} T_{M_C}\left(\frac{x}{y}, \frac{x+(q-1)y}{x-y}\right).$$

Most pedig írjuk fel, hogy a 3.3. Tétel szerint mivel egyenlő a jobb oldal.

$$\frac{1}{|C|} W_C(x + (q-1)y, x-y) = q^{-k}(x-y)^{n-k}(qy)^k T_{M_C}\left(\frac{qx}{qy}, \frac{x+(q-1)y}{x-y}\right).$$

Mivel az átalakított kifejezések megegyeznek, így a bal és a jobb oldal között valóban egyenlőség áll. □

3.3. A Tutte-polinomtól független kódparaméterek

A C lineáris kód tulajdonságainak és az M_C matroid Tutte-polinomjának kapcsolatát vizsgálva megállapítást nyert, hogy C számos tulajdonsága meghatározható T_{M_C} ismeretében. Peter Cameron tette fel a kérdést ([11], Problem 361), hogy vajon a lineáris térlefedő kódok elérési sugara is beletartozik-e ezekbe tulajdonságokba. A választ Thomas Britz és Carrie Rutherford adta meg [6], akik találtak két bináris mátrixot:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ és } \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

melyekhez tartozó mátrix-matroidoknak ugyanaz a Tutte-polinomja:

$$y^5+(x+5)y^4+(x^2+7x+12)y^3+(x^3+8x^2+22x+15)y^2+(2x^4+11x^3+27x^2+27x+7)y+$$
$$+(x^6+5x^5+13x^4+21x^3+19x^2+7x),$$

de az egyik 2, a másik 3 elérési sugarú kódot generál.

Ez alapján megfogalmazhatjuk a következő állítást:

3.8. Állítás. *A bináris lineáris térlefedő kódok elérési sugara nem mindig határozható meg a rajtuk vett matroid Tutte-polinomjából, azaz létezik olyan C_1 és C_2 bináris lineáris térlefedő kód, hogy $T_{M_{C_1}} = T_{M_{C_2}}$ és $R(C_1) \neq R(C_2)$.*

Azonban ennek az állításnak egy jóval erősebb verziója is igaz:

3.9. Tétel. *A lineáris térlefedő kódok elérési sugara nem mindig határozható meg a rajtuk vett matroidból, azaz létezik olyan C_1 és C_2 lineáris térlefedő kód, hogy $M_{C_1} = M_{C_2}$ és $R(C_1) \neq R(C_2)$.*

Bizonyítás. Mutatni fogunk egy ellenpéldát, azaz egy matroidnak megadjuk két olyan reprezentáló mátrixát, hogy az általuk generált kódok elérési sugara eltér. Legyen ez a matroid az $U_{3,6}$ uniform matroid, és a két $\mathbb{F}_7$-reprezentáció a következő:

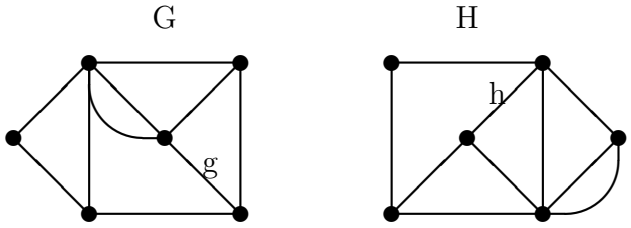
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 4 & 2 \end{pmatrix} \text{ és } \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 6 & 5 \end{pmatrix}.$$

Az első mátrix 2 elérési sugarú térlefedő kódot generál, a második pedig 3 elérési sugarút, így valóban nem igaz, hogy egy C lineáris kód elérési sugara mindig meghatározható az M_C matroidból. □

Definíció. Két gráfot *gyengén izomorfnak* vagy 2-*izomorfnak* nevezünk, ha létezik az élhalmazaik között körtartó bijekció.

3.10. Tétel. *Grafikus matroid Tutte-polinomja nem feltétlenül határozza meg gyenge izomorfia erejéig a reprezentáló gráfot.*

Bizonyítás. [42] Az úgynevezett Gray-gráfokra (1. ábra) teljesül, hogy a körmatroidjuk Tutte-polinomja megegyezik, de mégsem gyengén izomorfak.



1. ábra

Vegyük észre, hogy G-ből elhagyva g-t és H-ból elhagyva h-t izomorf gráfokat kapunk, csakúgy mint ha G-ben összehúzzuk g-t, illetve H-ban összehúzzuk h-t. Ez alapján a 3.1. Állításban mutatott rekurzióval igazolhatjuk a $T_{M[G]}$ és $T_{M[H]}$ polinomok egyenlőségét, míg a gyenge izomorfia sérüléséhez könnyen találhatunk olyan G-beli 6-hosszú kört, melynek H-ban nem 6-hosszú kör felel meg, hiszen G-ben több 6-hosszú kör (Hamilton-kör) van, mint H-ban.

□

A következő fejezetben megmutatjuk, hogy bár az 1. ábrán lévő gráfok gráfelméleti vágás-kódjain vett matroidok Tutte-polinomja is és a kódok elérési sugara is megegyezik, a WDCL mégis különböző.

4. Gráfelméleti kódok

Ebben a fejezetben irányítatlan gráfok által meghatározott kódokról (ú.n. gráfelméleti kódokról) adunk áttekintést [19]. Ezen kódok viszonylag könnyen dekódolhatóak és mind hibajavító mind térlefedő tulajdonságuk jól alkalmazható. Meghatározzuk a minimális távolságot matroidelméleti eszközökkel és ismertetjük, hogy az elérési sugár milyen gráfelméleti paraméternek felel meg. A Tutte-polinom kapcsán megmutatjuk, hogy két gráfelméleti kódnak megegyező Tutte-polinom és elérési sugár esetén is lehet különböző a WDCL-je. A kódok az itt leírttal analóg módon definiálhatóak több komponensű gráfok esetén is, de a legtöbb vizsgálat – és a bizonyítani kívánt tétel – összefüggő gráfból indul ki, ezért a fejezet erejéig feltesszük, hogy $G = (V, E)$ összefüggő, irányítatlan, n csúcsú és m élű gráf.

Definíció. A G gráf *rangja* (rank) a feszítőfáinak élszáma:

$$r(G) = n - 1,$$

nullitása (nullity) pedig a G feszítőfájának komplementerében lévő élek száma:

$$n(G) = m - n + 1.$$

Ez a rangfogalom egybevág a körmatroid rangjának meghatározásával: $r(G) = r(M[G])$.

Definíció. A G gráf *Euler-részgráfja* (Euler subgraph) alatt olyan részgráfot értünk, melyben minden csúcs foka páros. Könnyen meggondolható, hogy egy Euler-részgráf éldiszjunkt körök uniójából áll.

Definíció. Egy $\varnothing \neq X \subset V$ ponthalmazra az X és $V \setminus X$ között futó élek halmazát *vágásnak* (cut) nevezzük. Egy vágás *elemi* (bond), ha nem tartalmaz valódi részhalmazként másik vágást.

Jelölje S_B, ill. S_Q a G Euler-részgráfjainak, ill. vágásainak halmazát.

Válasszunk egy G-beli T feszítőfát és G éleit indexeljük a következőképp: $e_1, e_2, ..., e_{n(G)} \in E(\overline{T})$, $e_{n(G)+1}, e_{n(G)+2}, ..., e_m \in E(T)$. A fejezet végéig rögzítsük le ezt a T feszítőfát és az éleknek ezt a sorrendjét. Egy G' részgráf *él-karakterisztikus vektora* legyen az az $\mathbb{F}_2^m$-beli vektor, melynek i-edik komponense 1, ha $e_i \in E(G')$ és 0, ha $e_i \notin E(G')$.

Az S_B-beli, illetve S_Q-beli részgráfok él-karakterisztikus vektorai bináris lineáris kódot alkotnak (jelölje ezeket C_B, illetve C_Q), melyben a kódszavak hossza m. A kód dimenzióját kétféle megközelítéssel fogjuk keresni. Egyrészt ezekre a lineáris kódokra a szimmetrikus differencia képzés műveletével tekinthetünk úgy, mint $\mathbb{F}_2$ feletti vektorterekre, ahol a dimenzió nem más, mint a

vektortér egy bázisának elemszáma. Másrészt ha B, ill. Q az az $\mathbb{F}_2$ feletti $|S_B| \times m$-es, ill. $|S_Q| \times m$-es mátrix, melynek sorai az S_B-beli, ill. S_Q-beli részgráfok él-karakterisztikus vektorai, akkor a dimenzió megegyezik B, ill. Q rangjával.

Legyen b_i az az egyértelmű kör (alapkör), ami $e_i \in E(\overline{T})$ hozzávételével keletkezik $T_i = T \cup \{e_i\}$-ben ($i = 1, 2, ..., n(G)$). Készítsük el a $B^a \in \mathbb{F}_2^{n(G)\times m}$ *alapkör-mátrixot* a következőképp: az i-edik sor tartozzon az $e_i \in E(\overline{T})$ élhez, a j-edik oszlop pedig az $e_j \in E(G)$ élhez, és B^a i-edik sora legyen az e_i él alapkörének él-karakterisztikus vektora, vagyis

$$B^a{}_{ij} = \begin{cases} 1 & \text{, ha } e_j \text{ benne van } e_i \text{ alapkörében} \\ 0 & \text{, ha } e_j \text{ nincs benne } e_i \text{ alapkörében.} \end{cases}$$

4.1. Tétel. *A B^a mátrix a C_B kód egy generátormátrixa.*

Bizonyítás. Mivel B^a részmátrixa B-nek, és világos, hogy a sorvektorok lineárisan függetlenek (hiszen az első $n(G)$ oszlop egységmátrixot alkot), így csak azt kell belátni, hogy $r(B) = r(B^a) = n(G)$. Az $r(B) \geq n(G)$ irány következik abból, hogy az $n(G)$ rangú B^a mátrix részmátrixa B-nek. A másik irányhoz szükség lesz arra a megfigyelésre, hogy ha $A \in \mathbb{F}_2^{n\times m}$ a G gráf incidencia mátrixa (most is az élek fentebb rögzített sorrendje szerint), akkor AB^T a nullmátrix. Ez abból adódik, hogy az $(AB^T)_{ij}$ elem az A mátrix i-edik sorának és a B^T mátrix j-edik oszlopának (vagyis a B mátrix j-edik sorának) skaláris szorzata, és egy ilyen skaláris szorzat pontosan annyi darab egyes összege, ahány élre igaz, hogy illeszkedik a v_i csúcsra és benne van a G_j Euler-részgráfban. A definícióból következik, hogy egy Euler-részgráf éldiszjunkt körök uniója, így minden csúcsra csak páros sok olyan él illeszkedhet, ami benne van egy adott Euler-részgráfban, vagyis a modulo 2 számítás miatt az AB^T mátrixnak valóban minden eleme 0. Mivel tudjuk, hogy $r(A) = n - 1$ [23], a Sylvester-féle nullitás tétel [36] következő speciális alakjából adódik a tétel.

4.2. Lemma. *Ha $P \in \mathbb{F}^{p\times k}$ és $Q \in \mathbb{F}^{k\times q}$ olyan mátrixok, melyek szorzata a nullmátrix, akkor $r(P) + r(Q) \leq k$.*

A lemma bizonyítása. Jelöljük P rangját r-rel, és – ha szükséges – sor- és oszlopcserékkel alakítsuk át a P mátrixot úgy, hogy a bal felső sarkába egy $r\times r$-es nemszinguláris részmátrix (P_{11}) kerüljön, majd a P-beli oszlopcseréknek megfelelően rendezzük át Q sorait is:

$$P' = \begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix}, \quad Q' = \begin{pmatrix} Q_1 \\ Q_2 \end{pmatrix},$$

ahol Q_1 $r \times q$-as részmátrix. Így továbbra is fennáll, hogy $P'Q' = 0$, és $r(P') = r(P)$, $r(Q') = r(Q)$. A

$$\begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix}\begin{pmatrix} Q_1 \\ Q_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

mátrixszorzásból kapjuk, hogy $P_{11}Q_1 + P_{12}Q_2 = 0$, azaz $Q_1 + P_{11}^{-1}P_{12}Q_2 = 0$. Mivel nemszinguláris mátrix-szal való szorzás nem változtat a rangon, szorozzuk meg Q'-t balról az alábbi mátrixszal:

$$R = \begin{pmatrix} I_r & P_{11}^{-1}P_{12} \\ 0 & I_{k-r} \end{pmatrix}.$$

Így a

$$\begin{pmatrix} I_r & P_{11}^{-1}P_{12} \\ 0 & I_{k-r} \end{pmatrix}\begin{pmatrix} Q_1 \\ Q_2 \end{pmatrix} = \begin{pmatrix} Q_1 + P_{11}^{-1}P_{12}Q_2 \\ Q_2 \end{pmatrix} = \begin{pmatrix} 0 \\ Q_2 \end{pmatrix}$$

mátrixegyenletből adódik, hogy $r(Q') \leq k - r$, hiszen a jobb oldalon lévő mátrixnak csak $k - r$ nem azonosan nulla sora van. Ebből $r(Q) + r(P) \leq k$, vagyis a lemma állítását beláttuk. □

A lemmából kapjuk, hogy $r(A) + r(B^T) \leq m$, azaz $r(B) \leq m - (n-1) = n(G)$. Ezzel mindkét irányt beláttuk, B^a-ra valóban tekinthetünk a C_B kód generátormátrixaként, következésképp a C_B kód $n(G)$ dimenziós. □

Hasonlóan belátható, hogy a C_Q kód $r(G)$ dimenziós, és generátormátrixa az úgynevezett alapvágás-mátrix, ami alatt a következőt értjük. Legyen q_i az az egyértelmű vágás (alapvágás), amit az $e_i \in E(T)$, mint T-beli elvágó él határoz meg a csúcsok két részre partícionálásával: $V = V_1^i \dot{\cup} V_2^i$. A V_1^i és V_2^i között futó élek halmaza alkotja a q_i vágást $(i = n(G)+1, n(G)+2, ..., m)$. Készítsük el a $Q^a \in \mathbb{F}_2^{r(G)\times m}$ *alapvágás-mátrixot* a következőképp: az i-edik sor tartozzon az $e_i \in E(T)$ élhez, a j-edik oszlop pedig az $e_j \in E(G)$ élhez, és Q^a i-edik sora legyen az e_i él által meghatározott alapvágás él-karakterisztikus vektora, vagyis

$$Q^a{}_{ij} = \begin{cases} 1 & \text{, ha } e_j \text{ benne van a } q_i \text{ vágásban} \\ 0 & \text{, ha } e_j \text{ nincs benne a } q_i \text{ vágásban.} \end{cases}$$

A B^a mátrix által generált *kör-kódot* és Q^a mátrix által generált *vágás-kódot* szokás *gráfelméleti kódnak* nevezni.

4.3. Állítás. *A kör-kód és a vágás-kód – megegyező gráf esetén – egymás duálisai.*

Bizonyítás. Az állítás igazolásához azt kell megmutatnunk, hogy $B^a Q^{aT} = 0$, ami következik abból, hogy egy vágás egy kört csak páros sok élben metszhet. □

4.4. Következmény. *Q^a paritásellenőrző mátrixa a B^a mátrix által generált $C_B(m, n(G))$ kör-kódnak, és B^a paritásellenőrző mátrixa a Q^a által meghatározott $C_Q(m, r(G))$ vágás-kódnak.*

4.1. Hibajavító tulajdonság

A C_B, ill. a C_Q hibajavító gráfelméleti kód minimális távolsága a legrövidebb kör, ill. legkevesebb élből álló elemi vágás élszáma. Most csupán az 1.2. alfejezetben szereplő, matroidokra vonatkozó tételekkel bebizonyítjuk ezt az állítást a kör-kód esetén.

4.5. Tétel. *Legyen G összefüggő, n csúcsú, m élű gráf. Ekkor a G által generált C_B lineáris kód minimális távolsága megegyezik G legrövidebb körének élszámával.*

Bizonyítás. [28] Jelöljük d-vel a G legrövidebb körének hosszát. Az 1.16. Tétel szerint az $M[G]$ körmatroid köreinek halmaza megegyezik a G-beli körök élhalmazainak halmazával, tehát $M[G]$ legkisebb elemszámú köre d elemű. Az 1.17. Tétel alapján $M[G]$ minden test felett reprezentálható, így speciálisan $\mathbb{F}_2$-felett is. A vágások él-karakterisztikus vektoraiból, mint sorvektorokból álló Q mátrix a bináris $M[G]$ matroid egy $\mathbb{F}_2$-reprezentációja, de az 1.14. Megjegyzés szerint a Q-ból elemi sorekvivalens átalakításokkal kapott mátrixok, így a $Q^a \in \mathbb{F}_2^{r(G)\times m}$ mátrix is reprezentálja $M[G]$-t ($r(G) = r(M[G])$). Ekkor $M[G] \cong M[Q^a]$, amiből következik, hogy az $M[G]$-beli legkisebb elemszámú körnek és az $M[Q^a]$-beli legkisebb elemszámú körnek ugyanúgy d eleme van. Mivel a Q^a mátrix sorai lineárisan függetlenek, így a 2.5. Tétel miatt annak a kódnak, melyet a Q^a, mint paritásellenőrző mátrix határoz meg – vagyis a C_B kódnak – a minimális távolsága egyenlő az $M[Q^a]$-beli legkisebb elemszámú kör elemszámával, vagyis d-vel. □

4.2. Térlefedő tulajdonság

A gráfelméleti kódok térlefedő tulajdonságával kapcsolatban sokáig nem született jelentős eredmény, míg Ntafos és Hakimi 1981-ben a kínai postás problémára való átfogalmazás segítségével észrevette, hogy a gráfelméleti kódok könnyen dekódolhatóak ([32]). Az ehhez használt tételekből kiindulva Solé és Zaslavsky 1990-ben megmutatta, hogy az elérési sugár milyen gráfelméleti paraméternek felel meg ([40]), alsó korlátot adott az elérési sugárra összefüggő gráfok esetén és példaként hozott néhány gráfot, melyekre ez a korlát éles. Ezen átfogalmazás alapján Frank András ugyanebben az évben explicit formulát és polinomiális algoritmust adott a gráfelméleti kódok elérési sugarára ([15]).

Definíció. Ha T a $G = (V, E)$ gráf csúcsainak részhalmaza, akkor egy olyan $J \subseteq E$ részhalmazt, melyre teljesül, hogy minden $v \in T$ csúcsra $d_J(v)$ páratlan, $v \in V \setminus T$ esetén pedig $d_J(v)$ páros *T-kötésnek* (T-join) nevezünk. T-nek tehát szükségszerűen páros sok eleme van.

Jelölés. Jelölje $\tau_T(G)$ a G-beli minimális T-kötés elemszámát és

$$\tau(G) := \max_T \tau_T(G).$$

Definíció. Egy összefüggő gráfot akkor nevezünk *faktorkritikusnak*, ha bármely pontját kihagyva létezik teljes párosítása.

4.6. Tétel.

$$R(C_B) = \tau(G),$$

ahol $R(C_B)$ a G gráfon vett C_B kör-kód elérési sugarát jelöli.

4.7. Tétel.

$$R(C_B) = \frac{\varphi(G) + |V| - 1}{2},$$

ahol φ jelöli azon élek minimális számát, melyek összehúzásával a gráf faktorkritikussá válik.

Az előző fejezetben már említettük, hogy ha két lineáris térlefedő kód Tutte-polinomja és elérési sugara is megegyezik, abból még nem következik, hogy a két kód ekvivalencia erejéig meghatározott, hiszen a WDCL lehet eltérő. Példa erre az 1. ábrán látható két Gray-gráf vágás-kódja:
Ha $C_Q(G)$ jelöli a G gráf vágás-kódját, akkor $M_{C_Q(G)} = M[G]$ miatt a 3.10. Tétel bizonyítása szerint a Tutte-polinomok megegyeznek.
Mindkét kód elérési sugara 3, de $C_Q(G)$-hez az $1, 9, 20, 2$ WDCL, $C_Q(H)$-hoz pedig az $1, 9, 18, 4$ WDCL tartozik.

5. Szürjektív kódok

5.1. A téma ismertetése

A szürjektív kódok és az extremális halmazrendszerek kapcsolatával már foglalkoztunk a BSc-s szakdolgozatban is. Ott megmutattuk, hogy a 2-szürjektív bináris kódok és a páronként kvalitatív független halmazok rendszere tekinthető egymás egyfajta duálisának, és ennek segítségével adtunk egy rövid bizonyítást arra, hogy legfeljebb mennyi lehet az adott számú kódszóból álló bináris 2-szürjektív kódok dimenziószáma. Ebben a fejezetben további kapcsolatot mutatunk a szürjektív kódok és a kvalitatív független halmazok rendszerei között, valamint közöljük a tétel megértéséhez szükséges definíciókat. A kódelmélet ezen ágának alkalmazásaira itt nem térünk ki, de forrásként ajánljuk elsősorban Kéri Gerzson Optimális térlefedő kódok kutatása című akadémiai doktori értekezését [24]. A kvalitatív független halmazrendszerek vizsgálata nem csupán kódelméleti vonatkozásuk miatt fontos, hasznos eszköznek bizonyulnak a kereséselméletben is.

Definíció. Valamely $C \subseteq \mathbb{F}_q^n$ kód *s-szürjektív*, ha a tér koordinátáinak tetszőleges $\{a_1, a_2, ..., a_s\}$ halmazára, tetszőleges $(b_1, b_2, ..., b_s) \in \mathbb{F}_q^s$ választása esetén létezik legalább egy olyan $(c_1, c_2, ..., c_n) \in C$ kódszó, melyre fennáll $c_{a_i} = b_i$ minden i $(1 \leq i \leq s)$ esetén.
Vagyis egy kód pontosan akkor s-szürjektív, ha bármely s helyen bárhogy megadva a komponensek értékét, van legalább egy kódszó, ami illeszkedik az s darab előírt komponensre.

Definíció. Valamely $C \subseteq \mathbb{F}_q^n$ kód r *sugárral s-szürjektív*, ha a tér koordinátáinak tetszőleges $\{a_1, a_2, ..., a_s\}$ halmazára, tetszőleges $(b_1, b_2, ..., b_s) \in \mathbb{F}_q^s$ választása esetén létezik legalább egy olyan $(c_1, c_2, ..., c_n) \in C$ kódszó, melyre fennáll $c_{a_i} = b_i$ legalább $s - r$ számú i $(1 \leq i \leq s)$ esetén.
Vagyis egy kód pontosan akkor r sugárral s-szürjektív, ha bármely s helyen bárhogy megadva a komponensek értékét, van legalább egy kódszó, ami illeszkedik legalább $s - r$ helyen az előírt komponensekre.

Az r sugárral s-szürjektív kód Kéri Gerzson által bevezetett fogalma ([26], [25]) $r = 0$ esetén a hagyományos szürjektív kódot, $s = n$ esetén pedig a $\mathbb{F}_q^n$ Hamming-teret adja.

Vezessünk be külön elnevezést az r sugárral s-szürjektív kódok egy speciális esetére:

Definíció. Valamely $C \subseteq \mathbb{F}_q^n$ kód r *hiánnyal s-szürjektív*, ha a tér koordinátáiból alkotott tetszőleges $\{a_1, a_2, ..., a_s\}$ halmaznak van olyan $\{a'_1, a'_2, ..., a'_{s-r}\}$ részhalmaza, hogy tetszőleges $(b_1, b_2, ..., b_{s-r}) \in \mathbb{F}_q^{s-r}$ választása esetén létezik

legalább egy olyan $(c_1, c_2, ..., c_n) \in C$ kódszó, melyre fennáll $c_{a'_i} = b_i$ minden i $(1 \leq i \leq s-r)$ esetén.
Vagyis egy kód pontosan akkor r hiánnyal s-szürjektív, ha bármely s hely közül van $s-r$ olyan, hogy azokon bárhogy megadva a komponensek értékét, van legalább egy kódszó, ami illeszkedik az $s-r$ darab előírt komponensre.

Az r hiánnyal s-szürjektív kódok kielégítik az r sugárral s-szürjektív kódokra megfogalmazott feltételt, tehát valóban azok speciális esetéről van szó.

A szakirodalomban használt jelölés a q alapszámhoz tartozó n dimenziós s-szürjektív kódok méretének minimumára, illetve a q alapszámhoz tartozó n dimenziós, legfeljebb r sugárral s-szürjektív kódok méretének a minimumára:

$$\sigma_q(n, s), \text{ ill. } \sigma_q(n, s; r).$$

Ezek alapján vezessünk be egy új jelölést:

Jelölés. $\sigma_q(n, s; [r])$ jelölje a q alapszámhoz tartozó n dimenziós, legfeljebb r hiánnyal s-szürjektív kódok méretének minimumát.

A szürjektív kódok minimális méretére vonatkozóan egyelőre kevés pontos érték van meghatározva. Ezeket, illetve a legjobb ismert alsó és felső korlátokat $q \leq 8$, $n, s \leq 10$ (bináris kódokra $n, s \leq 14$) esetén megtalálhatjuk a [12] cikk tábázataiban.

Kimondunk két kódelméleti tételt és egy sejtést, melyek binomiális együtthatós formulával adják meg az adott számú kódszóból (n) álló egyes szürjektív bináris kódok dimenziószámának a maximális lehetséges értékét. A tételek halmazrendszeres duálisainak bizonyítására a 5.2. fejezetben, a kvalitatív független halmazok difiniálása után fogunk visszatérni.

5.1. Tétel. $\sigma_2(k, 2) = \min\left\{n : k \leq \binom{n-1}{\lfloor \frac{n-2}{2} \rfloor}\right\}$.

5.2. Tétel. *Ha m páratlan, akkor* $\sigma_2(k, m; [m-2]) = \min\left\{n : k \leq \Sigma(n, \left\lfloor \frac{m-1}{2} \right\rfloor)\right\}$.

5.3. Sejtés. *Ha m páros, akkor* $\sigma_2(k, m; [m-2]) = \min\left\{n : k \leq \Sigma\left(n; \left\lfloor \frac{m-1}{2} \right\rfloor\right) + \binom{n-1}{k-2}\right\}$, *ahol* $k = \min\left\{i : \binom{n}{i}\right.$ *szerepel* $\left.\Sigma\left(n; \left\lfloor \frac{m-1}{2} \right\rfloor\right)\right.$ *tagjai között*$\left.\right\}$.

5.2. Kvalitatív független halmazrendszerek

Ha egy szürjektív kód kódszavaira, mint sorvektorokra tekintünk, és őket egy mátrixba rendezzük, akkor a mátrix oszlopait értelmezhetjük egy halmazrendszer elemeinek karakterisztikus vektoraiként. Megvizsgálva, hogyan vihető át például a 2-szürjektivitás feltétele, épp a páronként kvalitatív független halmazrendszerekhez jutunk, az $m-2$ hiánnyal m-szürjektív kódokból pedig olyan halmazrendszereket kapunk, melyekre igaz, hogy bármely m elemből kiválasztható két kvalitatív független. Ennek a dualitásnak a bizonyítása

megtalálható a BSc-s szakdolgozatban, itt most nem részletezzük.

Definíció. *A és B kvalitatív független* halmazok, ha négyfelé vágják az alaphalmazt, vagyis ha $A \cap B$, $A \cap \overline{B}$, $\overline{A} \cap B$, $\overline{A} \cap \overline{B}$ egyike sem üres.

Jelölés. A továbbiakban $A * B$ jelölje azt, hogy A és B kvalitatív független halmazok.

Az 5.1. Tétel halmazrendszerekkel megfogalmazott alakja:

5.4. Tétel. *Legyen $\mathcal{A} = \{A_1, A_2, ..., A_k\}$ egy n elemű alaphalmaz páronként kvalitatív független halmazrendszere. Ekkor*

$$|\mathcal{A}| \leq \binom{n-1}{\lfloor \frac{n}{2} \rfloor - 1}.$$

Ennek a tételnek a bizonyítása megtalálható számos cikkben [5], [27], [3], [22], valamint körmódszert használva a BSc-s szakdolgozatomban is, ezért itt most nem részletezzük.

Definíció. Ha n és k egész számok, akkor jelölje $\Sigma(n,k)$ a k darab legnagyobb, n szerinti binomiális együttható összegét.

5.5. Tétel. *Legyen $\mathcal{A}$ olyan halmazrendszer egy n elemű alaphalmazon, amelyre teljesül, hogy bármely m eleme között biztosan van kettő, melyek kvalitatív függetlenek. Ekkor páratlan m esetén*

$$|\mathcal{A}| \leq \Sigma\left(n; \left\lfloor \frac{m-1}{2} \right\rfloor\right)$$

és ez a felső korlát elérhető.

Ez a tétel ekvivalens az előző fejezetben kimondott 5.2. Tétellel. Az $m = 3$ esetben a bizonyítás ismert [1], az alapján ezt az általánosabb alakot is a Katona Gyula által bevezetett körmódszerrel igazoljuk. Az intervallumrendszerre megfogalmazott lemmában tetszőleges m-re adunk felső becslést, nem használjuk ki, hogy m páratlan, de mint látni fogjuk páros m esetén a kettős leszámlálásból nem kapunk éles korlátot. A lemmához két bizonyítást közlünk, az első rövidebb, ötletigényes, míg a második mutatja, hogy a körmódszer használható mechanikusan, a rendelkezésre álló adatokból egyszerű számolásokkal is adódik a korlát, bár ennek az utóbbinak hátránya, hogy a páros és a páratlan esetet nem tudja együtt kezelni.

Bizonyítás. Vegyük észre, hogy $A_1 * A_2$ pontosan akkor teljesül, ha $A_1 * \overline{A}_2$. (Ez A_1 és A_2 kvalitatív függetlenségének definíciójából közvetlenül következik.) Ezt szeretnénk kihasználni és az $\frac{n}{2}$-nél nagyobb elemszámú halmazok helyett

a komplementerüket nézni, de hogy elkerüljük a többszörös multiplicitást, egy halmaz helyett csak akkor vesszük a komplementerét, ha az még nem eleme a halmazrendszernek. Így elérhető, hogy minden $A \in \mathcal{A}$ halmazra vagy $|A| \leq \left\lfloor \frac{n}{2} \right\rfloor$ vagy $\overline{A} \in \mathcal{A}$.

5.6. Lemma. *Vegyük az n elem egy ciklikus permutációját $(\sigma(1), \sigma(2), ..., \sigma(n))$ és ezen egy $\mathcal{B}$ intervallumrendszert ($\forall B \in \mathcal{B}$: $1 \leq |B| \leq \left\lfloor \frac{n}{2} \right\rfloor$ vagy $\overline{B} \in \mathcal{B}$), melyre teljesül, hogy bármely m intervalluma közül kiválasztható kettő, ami kvalitatív független. Ekkor*

$$|\mathcal{B}| \leq \left\lfloor \frac{(m-1)n}{2} \right\rfloor.$$

A lemma bizonyítása. Egy $B \in \mathcal{B}$ intervallumot nevezzünk *rövidnek*, ha $|B| \leq \left\lfloor \frac{n}{2} \right\rfloor$ és *hosszúnak*, ha $|B| > \frac{n}{2}$. A feltevés szerint minden $\mathcal{B}$-beli hosszú intervallum (rövid) komplementere is $\mathcal{B}$-ben van.
Egy elemmel nem kezdődhet $m-1$-nél több intervallum, mert ha lenne $\mathcal{B}$-nek m olyan eleme, melyek mindegyike $\sigma(i)$-ből indul, akkor közülük bárhogy választunk ki két intervallumot, az egyik tartalmazni fogja a másikat, és tartalmazás esetén nem teljesül a kvalitatív függetlenség. Tehát $|\mathcal{B}| \leq (m-1)n$, de ezt a felső korlátot még tovább csökkentjük.

Legyen $\mathcal{L}_1(\sigma(i))$ a $\sigma(i)$-ből induló rövid intervallumok halmaza, $\mathcal{L}_2(\sigma(i))$ pedig a $\sigma(i)$-ből induló rövid intervallumok $\mathcal{B}$-beli komplementereinek halmaza. (Világos, hogy ekkor $\forall B \in \mathcal{L}_2(\sigma(i)) : \overline{B} \in \mathcal{L}_1(\sigma(i))$.) Vezessük be a következő jelölést: $l_{\sigma(i)} := |\mathcal{L}_1(\sigma(i))| + |\mathcal{L}_2(\sigma(i))|$, és mutassuk meg, hogy

$$l_{\sigma(i)} + l_{\sigma(i)+\lfloor \frac{n}{2} \rfloor} \leq m-1, \quad \forall i = 1, 2, ..., n,$$

az indexeket modulo n értve.

Ehhez azt kell belátnunk, hogy az $\mathcal{L}_1(\sigma(i)) \cup \mathcal{L}_1(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor) \cup \mathcal{L}_2(\sigma(i)) \cup \mathcal{L}_2(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor)$ intervallumrendszernek nincs két kvalitatív független eleme, így a mérete legfeljebb $m-1$ lehet. Vizsgáljuk meg a lehetséges eseteket!

1. $\mathcal{L}_1(\sigma(i))/\mathcal{L}_2(\sigma(i))/\mathcal{L}_1(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor)/\mathcal{L}_2(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor)$ elemei közül bármely kettőre igaz, hogy egyik tartalmazza a másikat.

2. $\forall B \in \mathcal{L}_1(\sigma(i)), B' \in \mathcal{L}_2(\sigma(i)) : B \cap B' = \varnothing$ vagy $\overline{B} \cap \overline{B'} = \varnothing$.

3. $\forall D \in \mathcal{L}_1(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor), D' \in \mathcal{L}_2(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor) : D \cap D' = \varnothing$ vagy $\overline{D} \cap \overline{D'} = \varnothing$.

4. $\forall B \in \mathcal{L}_1(\sigma(i)), D \in \mathcal{L}_1(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor) : B \cap D = \varnothing$, mert B és D rövid intervallumok.

5. $\forall B' \in \mathcal{L}_2(\sigma(i)), D' \in \mathcal{L}_2(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor) : \overline{B'} \cap \overline{D'} = \varnothing$, mert B' és D' hosszú intervallumok.

6. $\forall B \in \mathcal{L}_1(\sigma(i)), D' \in \mathcal{L}_2(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor) : B \subseteq D'$.

7. $\forall D \in \mathcal{L}_1(\sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor), B' \in \mathcal{L}_2(\sigma(i)) : D \subseteq B'$.

Mivel ezzel az összes lehetséges halmazpárt megvizsgáltuk, valóban megkaptuk, hogy $l_{\sigma(i)} + l_{\sigma(i)+\lfloor \frac{n}{2} \rfloor} \leq m-1, \quad \forall i = 1, 2, ..., n$.

Ezt felhasználva felső korlátot tudunk adni $|\mathcal{B}|$-re:

$$|\mathcal{B}| = \sum_{i=1}^{n} l_{\sigma(i)} = \frac{1}{2} \sum_{i=1}^{n} (l_{\sigma(i)} + l_{\sigma(i)+\lfloor \frac{n}{2} \rfloor}) \leq \frac{1}{2}(m-1)n,$$

következésképpen

$$|\mathcal{B}| \leq \left\lfloor \frac{(m-1)n}{2} \right\rfloor.$$

□

Másik bizonyítás a lemmára. Ha vesszük azon elemek halmazát, amikre $|\mathcal{L}_1| + |\mathcal{L}_2| = m-1$: $A_{m-1} \subseteq \{\sigma(1), \sigma(2), ..., \sigma(n)\}$ és azon elemek halmazát, melyekkel nem kezdődik egy rövid intervallum se: $A_0 \subseteq \{\sigma(1), \sigma(2), ..., \sigma(n)\}$, akkor $\exists \varphi_0 : A_{m-1} \to A_0, \quad \varphi_0(\sigma(i)) = \sigma(i) + \left\lfloor \frac{n}{2} \right\rfloor$, amire $\varphi_0(\sigma(i)) \neq \varphi_0(\sigma(i'))$ ha $\sigma(i) \neq \sigma(i')$. Ezért $|A_0| \geq |A_{m-1}|$, vagyis legalább annyi elemből nem indulhat rövid intervallum (legalább annyi elemre teljesül az $|\mathcal{L}_1| + |\mathcal{L}_2| = 0$ egyenlőség), mint amennyire fennáll, hogy $|\mathcal{L}_1| + |\mathcal{L}_2| = m-1$.

Hasonló megfontolásból adódik, hogy $\exists \varphi_j : A_{m-1-j} \to \bigcup_{i=0}^{j} A_i, \quad \varphi_j(\sigma(l)) = \sigma(l) + \left\lfloor \frac{n}{2} \right\rfloor$, amire $\varphi_j(\sigma(l)) \neq \varphi_j(\sigma(l'))$ ha $\sigma(l) \neq \sigma(l')$, $\forall j = 0, 1, ..., \left\lfloor \frac{m}{2} \right\rfloor - 1$, ahol $A_i \subseteq \{\sigma(1), \sigma(2), ..., \sigma(n)\}$ jelöli azon elemek halmazát, amelyekre a belőle induló rövid intervallumok száma plusz azoknak a belőle induló rövid intervallumoknak a száma, melyek komplementere is $\mathcal{B}$-beli épp i. Vagyis egy olyan $\sigma(l)$ elem esetén, melyre $l_{\sigma(l)} = m-1-j, \quad \sigma(l) + \left\lfloor \frac{n}{2} \right\rfloor$ egy olyan pont, amire $l_{\sigma(l)+\lfloor \frac{n}{2} \rfloor} \leq j$. Így kapjuk, hogy $\sum_{i=0}^{j} |A_i| \geq |A_{m-1-j}|$, $\forall j = 0, 1, ..., \left\lfloor \frac{m}{2} \right\rfloor - 1$.

De a $\sum_{i=0}^{j} |A_i|$ értékekre erősebb alsó becslés is kiolvasható az eddigiekből:

$$\sum_{i=0}^{j} |A_i| \geq \sum_{i=0}^{j} |A_{m-1-i}|, \quad \forall j = 0, 1, ..., \left\lfloor \frac{m}{2} \right\rfloor - 1.$$

Jelöljük a_i-vel az A_i halmaz elemszámát, és írjuk fel az ismert összefüggéseket!

$$\sum_{i=0}^{m-1} a_i = n, \quad |\mathcal{B}| = \sum_{i=0}^{m-1} i \cdot a_i$$

az A_i halmazok definiálása miatt nyilvánvaló, a

$$\sum_{i=0}^{j} a_{m-1-i} \leq \sum_{i=0}^{j} a_i \quad \left(i = 0, 1, ..., \left\lfloor \frac{m}{2} \right\rfloor - 1\right)$$

egyenlőtlenségeket pedig épp az előbb láttuk be. Ezeket összevetve páratlan m esetén ($m = 2k + 1$ valamely k egész számra) kapjuk, hogy

$$|\mathcal{B}| = \sum_{i=0}^{2k} i \cdot a_i = k\left(\sum_{i=0}^{2k} a_i\right) + \sum_{i=0}^{2k} (i-k)a_i = kn + \sum_{i=0}^{k-1} (k-i)a_{2k-i} - \sum_{i=0}^{k-1} (k-i)a_i =$$

$$kn + \sum_{j=o}^{k-1}\left(\sum_{i=0}^{j} a_{2k-i}\right) - \sum_{j=o}^{k-1}\left(\sum_{i=0}^{j} a_i\right) \leq$$

$$\leq kn + \sum_{j=o}^{k-1}\left(\sum_{i=0}^{j} a_i\right) - \sum_{j=o}^{k-1}\left(\sum_{i=0}^{j} a_i\right) = kn = \left\lfloor \frac{m-1}{2} \right\rfloor n$$

Ha m páros ($m := 2k$ valamely k egész számra), akkor a $k \cdot n$ felső korlát nem elég erős a lemma bizonyításához, még tovább kell szigorítani:

$$|\mathcal{B}| = \sum_{i=0}^{2k-1} i \cdot a_i = k\left(\sum_{i=0}^{2k-1} a_i\right) + \sum_{i=0}^{2k-1} (i-k)a_i = kn + \sum_{i=0}^{k-1} (k-1-i)a_{2k-1-i} - \sum_{i=0}^{k-1} (k-i)a_i =$$

$$= kn + \sum_{j=0}^{k-2}\left(\sum_{i=0}^{j} a_{2k-1-i}\right) - \sum_{j=0}^{k-1}\left(\sum_{i=0}^{j} a_i\right) \leq kn + \sum_{j=0}^{k-2}\left(\sum_{i=0}^{j} a_i\right) - \sum_{j=0}^{k-1}\left(\sum_{i=0}^{j} a_i\right) =$$

$$= kn + \sum_{i=0}^{k-2} (k-1-i)a_i - \sum_{i=0}^{k-1} (k-i)a_i = kn + \sum_{i=0}^{k-1} (k-1-i)a_i - \sum_{i=0}^{k-1} (k-i)a_i = kn - \sum_{i=0}^{k-1} a_i$$

Ahhoz, hogy ezt tovább becsülhessük felülről, meg kell adnunk $\sum_{i=0}^{k-1} a_i$ egy alsó korlátját:

$$\sum_{i=0}^{2k-1} a_i = n \rightarrow \quad n \leq 2 \cdot \sum_{i=0}^{k-1} a_i \rightarrow \quad \frac{n}{2} \leq \sum_{i=0}^{k-1} a_i \rightarrow \quad \left\lceil \frac{n}{2} \right\rceil \leq \sum_{i=0}^{k-1} a_i,$$

mert az a_i-k nemnegatív egész számok.

Tehát itt is azt kaptuk, hogy

$$|\mathcal{B}| \leq kn - \sum_{i=0}^{k-1} a_i \leq kn - \left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{2kn - n}{2} \right\rfloor = \left\lfloor \frac{(m-1)n}{2} \right\rfloor,$$

amivel a lemma állítását beláttuk minden $m \geq 2$ egész számra. □

Térjünk vissza a tétel bizonyítására.
Vizsgáljuk kettős leszámlálást alkalmazva a (C, A) párok számát, ahol C az n elem egy ciklikus permutációja, $A \in \mathcal{A}$ pedig egy intervallum a permutált elemeken.
Először tekintsük A-t rögzítettnek. Mivel A és $\overline{A}$ elemei egymástól függetlenül permutálhatóak, azon ciklikus permutációk száma, amiknél A intervallum marad: $|A|!(n-|A|)!$. Tehát a (C, A) párok száma $\sum_{A \in \mathcal{A}} |A|!(n-|A|)!$.
Most rögzítsük a C permutációt. Az n elemnek $(n-1)!$ különböző ciklikus permutációja van, és mivel a C szerinti intervallumokra teljesül, hogy bármely m közül kiválasztható kettő, ami kvalitatív független, a lemma mindegyikre alkalmazható, vagyis a (C, A) párok száma legfeljebb $\left\lfloor \frac{(m-1)n}{2} \right\rfloor \cdot (n-1)!$.
Felhasználva, hogy m páratlan, a két leszámlálás összehasonlításából kapjuk:

$$\sum_{A \in \mathcal{A}} |A|!(n-|A|)! \leq \left\lfloor \frac{(m-1)n}{2} \right\rfloor (n-1)! = \left\lfloor \frac{m-1}{2} \right\rfloor n!.$$

Osszuk le az egyenlőtlenséget $n!$-sal:

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{n}{|A|}} \leq \left\lfloor \frac{m-1}{2} \right\rfloor.$$

A bal oldal értéke annál kisebb lesz, minél közelebb van az $\mathcal{A}$-beli halmazok mérete $\frac{n}{2}$-höz, vagyis akkor lesz minimális, ha kiválasztjuk az összes $\left\lfloor \frac{n}{2} \right\rfloor$, $\left\lceil \frac{n}{2} \right\rceil$ elemszámú halmazt, és utána mindig az eggyel kisebb/nagyobb elemszámú halmazokat vesszük be, amíg lehetséges.
Így azt kapjuk, hogy

$$|\mathcal{A}| \leq \Sigma\left(n; \left\lfloor \frac{m-1}{2} \right\rfloor\right),$$

és ez a felső becslés tovább nem javítható, ugyanis a $\Sigma\left(n; \left\lfloor \frac{m-1}{2} \right\rfloor\right)$ darab $\frac{n}{2}$-höz legközelebbi halmazt véve egyenlőséget kapunk, és ez a halmazrendszer valóban m-kvalitatív független lesz. □

Páros m-ekre a lemmából kapott korlát sajnos nem éles:

$$\sum_{A \in \mathcal{A}} |A|!(n-|A|)! \leq \left\lfloor \frac{(m-1)n}{2} \right\rfloor (n-1)! = \left(\left\lfloor \frac{m-1}{2} \right\rfloor \cdot n + \left\lfloor \frac{n}{2} \right\rfloor \right) (n-1)!.$$

Leosztva az egyenlőtlenséget $n!$-sal:

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{n}{|A|}} \leq \left\lfloor \frac{m-1}{2} \right\rfloor + \frac{\left\lfloor \frac{n}{2} \right\rfloor}{n},$$

amiből

$$|\mathcal{A}| \le \Sigma\left(n; \left\lfloor \frac{m-1}{2} \right\rfloor\right) + \binom{n-1}{\lfloor \frac{n}{2} \rfloor - 1}.$$

Behelyettesítve $m = 2$ esetén valóban adódik az 5.4. Tétebeli felső korlát, nagyobb páros m-ekre viszont ez egy kicsit gyenge becslés.

5.7. Sejtés. *Legyen $\mathcal{A}$ olyan halmazrendszer egy n elemű alaphalmazon, amelyre teljesül, hogy bármely m eleme között biztosan van kettő, melyek kvalitatív függetlenek. Ekkor páros m esetén*

$$|\mathcal{A}| \le \Sigma\left(n; \left\lfloor \frac{m-1}{2} \right\rfloor\right) + \binom{n-1}{k-2},$$

ahol $k = \min\{i : \binom{n}{i}$ szerepel $\Sigma\left(n; \lfloor \frac{m-1}{2} \rfloor\right)$ tagjai között$\}$.

Hivatkozások

[1] B. Barbara, Kvalitatíve majdnem-független halmazok, *Matematikai Lapok* **2**, 2012.

[2] Michael Barany honlapján:
http://www.math.umn.edu/~reiner/Tutte/TUTTE.html

[3] B. Bollobás, Sperner systems consisting of pairs of complementary subsets, *J. Combinatorical Theory* ser.**A** vol.**15**, 1973, 363-366.

[4] Iliya Bouyukliev, Irina Gancheva, A method for calculation the weight distribution of the coset leaders of a linear code, *notes*, Institute of Mathematics and Informatics Bulgarian Academy of Sciences

[5] A. Brace, D.E. Daykin, Sperner type theorems for finite sets, *Combinatorics*, 1972, 18-37.

[6] T. Britz, C.G. Rutherford, Covering radii are not matroid invariants, *Discrete Math.* **296**, 2005, 117-120.

[7] T. Britz, Extensions of the Critical Theorem, *Discrete Math.* **305**, 2005, 55-73.

[8] Thomas Britz honlapja: http://www.thomasbritz.dk/

[9] P.J. Cameron, Notes on matroids and codes, *expository article*

[10] P.J. Cameron, Polynomial aspects of codes, matroids and permutation groups, *lecture notes*, 2002.

[11] P.J. Cameron, Research problems, *Discrete Math.* 231, 2001, 469 – 478.

[12] C. J. Colbourn, G. Kéri, P. P. Rivas Soriano, J.-C. Schlage-Puchta, Covering and radius-covering arrays: constructions and classification, *Discrete Appl. Math.*, 1948.

[13] H. Crapo, The Tutte polynomial, *Aequationes Math.* **3**, 1969, 211-229.

[14] H. Crapo, G.-C. Rota, On the Foundations of of Combinatorial Theory: Combinatorial Geometries, *MIT Press*, Cambridge, MA, London, 1970.

[15] A. Frank, Conservative weightings and ear-decompositions of graphs, *Combinatorica* **13**, 1993, 65-81.

[16] Frank András, Kombinatorikus optimalizálás II.: Matroidelmélet, *egyetemi jegyzet*, Eötvös Loránd Tudományegyetem, 2011.

[17] Curtis Greene, Weight Enumeration and the Geometry of Linear Codes, *Stud. Appl. Math.* **55**, 1976, 119-128.

[18] S.L. Hakimi, J.G. Bredeson, Graph Theoretic Error-Correcting Codes, *IEEE Trans. Inform. Theory* **14**, 1968, 584-591.

[19] S.L. Hakimi, H. Frank, Cut-Set Matrices and Linear Codes, *IEEE Trans. Inform. Theory* **11**, 1965, 457.

[20] Ivanyos Gábor, Algebrai kódelmélet, *egyetemi jegyzet*, Budapesti Műszaki és Gazdaságtudományi Egyetem, 2009.
http://www.math.bme.hu/~ig/regikod/vazlat.pdf

[21] Navin Kashyap, Applications of Matroid Methods to Coding Theory, *BIRS Workshop*, 2009.

[22] G. O. H. Katona, Two applications (for search theory and truth functions) of Sperner type theorems, *Period. Math. Hungar.* **3**, 1973, 19-26.

[23] Katona Y. Gyula, Recski András, Szabó Csaba, A számítástudomány alapjai, *Typotex kiadó*, Ötödik kiadás, 2006.

[24] Kéri Gerzson, Optimális térlefedő kódok kutatása, *Akadémiai doktori értekezés, MTA*, 1972.

[25] G. Kéri, P.R.J. Östergård, Bounds for covering codes over large alphabets, *Des. Codes Cryptogr.* **137**, 2005.

[26] G. Kéri, P.R.J. Östergård, On the covering radius of small codes, *Studia Sci. Math. Hungar.* **40**, 2003, 243-256.

[27] D.J. Kleitman, J. Spencer, Families of k-independent sets, *Discrete Math.* **6**, 1973, 255-262.

[28] G.G. La Guardia, L. Grossi, R.C.A. Vieira, M.A.V. Pinto, A note on matroids, codes and information theory, *International Journal of Pure and Applied Mathematics*, vol. **70**, no. **3**, 2011, 307-316.

[29] Lakatos Piroska, Kódelmélet, *egyetemi jegyzet*, Debreceni Egyetem, 2010.

[30] F.J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell System Tech. J.* **42**, 1963, 79-94.

[31] Criel Merino, Marcelino Ramírez-Ibañez, Guadalupe Rodríguez-Sánchez The Tutte polynomial of some matroids, *expository article*, 2012.

[32] S.C. Ntafos, S.L. Hakimi, On the Complexity of Some Coding Problems, *IEEE Trans. Inform. Theory*, vol. **27**, no. **6**, 1981, 794-796.

[33] J. Oxley, Matroid Theory, *Oxford University Press*, New York, 1992.

[34] David J. Pearce honlapján: http://homepages.mcs.vuw.ac.nz/~djp/tutte/

[35] W.W. Peterson, E.J. Weldon, Error-Correcting Codes, *MIT Press*, Second edition, 1996.

[36] Rózsa Pál, Lineáris Algebra és alkalmazásai, Harmadik kiadás, *Tankönyvkiadó*, Budapest, 1991.

[37] M. Schönert, et al., GAP–Groups, Algorithms and Programming, fifth ed., Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, 1995.

[38] A.N. Skorobogatov, Linear codes, strata of Grassmannians, and the problems of Segre, *Coding Theory and algebraic geometry, Proc. Int. Workshop*, Luminy/France 1991, *Lect. Notes Math.* **1518**, 1992, 210-223.

[39] Sundaram Seshu, Myril B. Reed, Linear Graphs and Electrical Networks, *Addison-Wesley Publishing Company*, 1961.

[40] P. Solé, T. Zaslavsky, The covering radius of the cycle code of a graph, *Discrete Applied Mathematics* **45**, 1993, 63-70.

[41] The Magma Computational Algebra System for Algebra, Number Theory and Geometry: http://magma.maths.usyd.edu.au/magma/

[42] W.T. Tutte, Codichromatic graphs, *J. Combin. Theory*, Ser. B **16**, 1974, 168-174.

[43] D.J.A. Welsh, Matroid Theory, *Academic Press*, London, 1976.