Titokmegosztás és a bonyolultság vizsgálata gráfokon

Szakdolgozat

Harsányi Károly

Matematika BSc
Elemző szakirány

Témavezető:

dr. Ligeti Péter, adjunktus
Komputeralgebra Tanszék
Eötvös Loránd Tudományegyetem, Informatikai Kar

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2015

Tartalomjegyzék

Bevezetés

A titokmegosztás a kriptográfia fontos területe, amely sok megoldatlan problémával kecsegtet. Szakdolgozatomban a titokmegosztás témakörén belül, elsősorban gráfok bonyolultságának/információs hányadosának vizsgálatával foglalkozom.

Az első fejezetekben ismertetem a titokmegosztás problémakörét, definiálom az alapfogalmakat, valamint leírom Shamir és Blakley titokmegosztási sémáinak működését. Ezután a bonyolultság becslésére szolgáló alsó és felső korlátok meghatározásra alkalmas technikákat ismertetem, és bemutatok olyan gráfcsaládokat, amelyeknek bonyolultságát valamilyen módon már megállapították.

Később leírok 117 kisméretű gráfot, amelyek bonyolultságát lineáris programozás segítségével meghatároztam. A felsorolt gráfok közül számos még nem szerepelt egy publikációban sem, valamint nem tagja egyetlen ismert bonyolultságú gráfcsoportnak sem.

Végül egy olyan új, eddig még nem publikált, végtelen gráfcsaládot definiálok, amely bonyolultságát csillagfedések és az információ elméleti módszer segítségével sikerült meghatároznom.

1. fejezet

Titokmegosztás alapjai

A titokmegosztás vezérgondolata a következő: egy úgynevezett osztó (*dealer*) szétoszt egy titkot n (véges sok) résztvevő között úgy, hogy a résztvevőknek csak bizonyos meghatározott részhalmazai tudják megfejteni a titkot a rendelkezésükre álló részekből, a résztvevők többi részhalmaza azonban erre nem képes.

Például egy széf kinyitásához két különböző kulcsra van szükség és ezeket két különböző ember birtokolja, így tehát a széf tartalmához csak akkor férhetnek hozzá, ha mindketten jelen vannak.

A következő szekcióban definiálom, majd pár egyszerű példával illusztrálom a titokmegosztás néhány alapfogalmát az [1] alapján.

1.1. Definíciók

Legyen P a résztvevők véges halmaza: $P = \{v_1, v_2, \ldots, v_n\}$. $\xi, \xi_1, \xi_2, \ldots, \xi_n$ pedig $n+1$ darab (azonos eloszlással rendelkező) valószínűségi változó. A ξ értéke a *titok*, $\xi_1, \xi_2, \ldots, \xi_n$ értéke pedig az n darab *titokrész*. A ξ_i értékét egyedül a v_i résztvevő ismeri.

Definíció 1.1.1 (Elérési struktúra) *A résztvevők részhalmazainak egy α családja elérési struktúra, amennyiben teljesül a következő feltétel: ha $A \in \alpha$ és $A \subseteq B$, akkor $B \in \alpha$.*

Informálisan azt mondjuk, hogy egy $(\xi, \xi_1, \ldots \xi_n)$ megvalósítja α-t, ha az $A \in \alpha$ részhalmazok tagjai meg tudják határozni a titok értékét (ezeket a részhalmazokat nevezzük *kvalifikált részhalmazoknak*), a $B \notin \alpha$ részhalmazok, (vagyis a *nem kvalifikált részhalmazok*) azonban erre nem képesek. A formális definíció a következő:

Definíció 1.1.2 (Tökéletes titokmegosztás) *Legyen α a résztvevők részhalmazainak egy családja. Ekkor $(\xi, \xi_1, \ldots, \xi_n)$ az α-t megvalósító tökéletes titokmegosztás, ha*

(i) $\forall A \in \alpha$ *esetén* $\{\xi_a : a \in A\}$ *meghatározza* ξ*-t*

(ii) $\forall B \notin \alpha$ *esetén* $\{\xi_b : b \in B\}$ *független* ξ*-től.*

1.1.1. Példa 1

ξ_1	0	0	0	1	1	1	2	2	2
ξ_2	0	1	2	0	1	2	0	1	2
ξ_3	0	2	1	2	1	0	1	0	2
ξ	0	1	2	2	0	1	1	2	0

1.2.1.1 táblázat

Az 1.2.1.1 táblázat oszlopaiban a három titokrész és a titok lehetséges együttes értékei vannak feltüntetve. Minden oszlop 1/9 valószínűséggel fordul elő. Könnyű ellenőrizni, hogy például ξ_1 és ξ függetlenek, mivel mind a kilenc lehetőség pontosan egyszer fordul elő. Hasonlóan ξ_2 és ξ valamint ξ_3 és ξ is függetlenek. Tehát az egyelemű részhalmazok nem kvalifikáltak. Ugyanakkor bármely két résztvevő együttes értéke már egyértelműen meghatározza a ξ-t, vagyis a titok értékét. Következésképpen bármely kételemű részhalmaz kvalifikált lesz (és természetesen a kettőnél nagyobb elemszámú részhalmazok is kvalifikáltak).

Definíció 1.1.3 ((n, k) küszöbséma) *Tegyük fel, hogy az osztó a titkot n részre osztja, és teljesülnek a következő feltételek:*

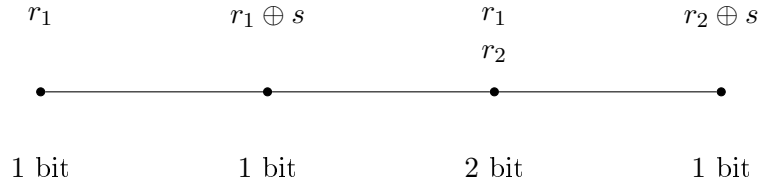
(i) bármely k vagy több titokrész elegendő a titok kiszámításához

(ii) bármely $k-1$ vagy kevesebb titokrész független a titok értékétől.

A fenti példában szereplő séma, értelemszerűen $(3, 2)$ küszöbséma.

1.1.2. Példa 2 - A három hosszú út

Elérési struktúrákat gráfok segítségével is megadhatunk úgy, hogy a gráf csúcsai a résztvevők, és a csúcsok egy részhalmaza akkor és csak akkor kvalifikált ha az általuk feszített részgráf legalább 1 élt tartalmaz. A következő példában három élből és négy csúcsúból álló vonalgráfon fogunk a titokmegosztás végezni. A titok legyen egy véletlenszerűen választott s bit, valamint legyenek r_1 és r_2 szintén egy véletlen bitek. Tehát $s, r_i \in \{0, 1\}$. Jelölje $\oplus$ a modulo kettő összeadást. A következő ábra mutatja, hogy az egyes résztvevők milyen információt jegyeznek meg:

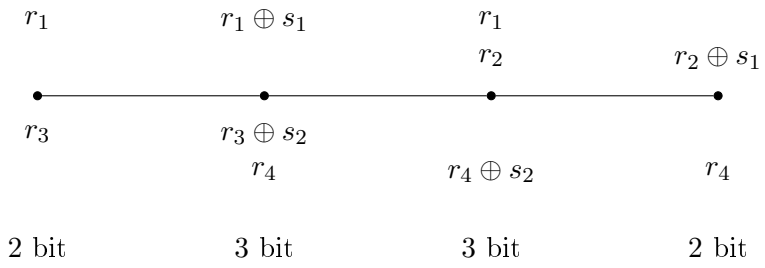


1.2.2.1 ábra: Titokmegosztás a 3 hosszú úton

A szomszédos résztvevők meg tudják fejteni a titkot, hiszen az általuk birtokolt bitek modulo 2 összege egyenlő a titokkal. A harmadik résztvevőnek két bitet kell megjegyeznie

ahhoz, hogy a titkot mindkét szomszédjával meg tudja fejteni. A nem kvalifikált részhalmazoknak (független csúcshalmazoknak) semmilyen információjuk nincs a titokról.

A szétosztás szimmetrikussá tehető, ha titok méretét 2 bitre növeljük. Az ily módon történő szétosztást az 1.2.2.2 ábra szemlélteti:



1.2.2.2 ábra: Szimmetrizálás

Ebben az esetben tehát a két belső résztvevő 3-3 bit információt jegyez meg, a két szélső pedig 2-2 bitet. Ez azt jelenti, hogy minden résztvevőnek legfeljebb a titok másfélszeresét kell megjegyeznie, ellenben a korábban vizsgált esettel, ahol egy résztvevő a titokban lévő információmennyiség kétszeresét kellett, hogy tárolja.

Az, hogy egy adott sémában az egyes résztvevőknek mekkora adatmennyiséget kell tárolniuk a titok eredeti méretéhez képest, fontos és nem feltétlenül egyszerű kérdés, amivel a későbbi fejezetekben foglalkozom.

2. fejezet

Küszöbsémák

2.1. Shamir titokmegosztási módszere

Shamir titokmegosztási módszere [2] polinomok interpolációján alapul: adva van k darab $(x_1, y_1) \dots (x_k, y_k)$ pont a 2 dimenziós térben úgy, hogy minden x_i különböző. Ekkor pontosan egy olyan $k-1$ fokú $q(x)$ polinom létezik, hogy $q(x_i) = y_i$ minden i-re. Az általánosság elvesztése nélkül feltételezhetjük, hogy a titok amit szétosztunk valamilyen D számmal reprezentálható. A D értéke csak az osztó számára ismert. Tetszőlegesen választunk $a_1, \dots a_{k\text{-}1}$ együtthatókat egy $k-1$ fokú $q(x) = a_0 + a_1 x + \dots + a_{k\text{-}1} x^{k-1}$ polinomhoz, a_0 pedig legyen egyenlő D-vel. Az i-edik résztvevő titokrésze legyen D_i. Ezeket a következő módon számolhatjuk ki: $D_1 = q(1), D_2 = q(2), \dots, D_n = q(n)$. Bármely k van a birtokunkban az ilyen módszerrel megadott D_i-k közül, interpoláció segítségével megfejthetjük a titkot. Másrészt viszont $k-1$ titokrész nem elegendő D értékének kiszámolásához.

Ahhoz, hogy pontosítsuk a fenti állítást, az interpolációt egy modulo p (p valamilyen prím) számhalmazon hajtjuk végre. Válasszuk p-t úgy, hogy a D-nél és n-nél is nagyobb legyen. A $q(x)$ polinomhoz $a_1, \dots, a_{k\text{-}1}$ együtthatókat véletlenszerűen választjuk a $[0, p)$ egészek közül (mindet ugyanolyan valószínűséggel), továbbá a $D_1, \dots, D_n$ értékeket is modulo p szerint számoljuk ki.

Tegyük fel, hogy $k-1$ darab ezek közül a $D_1, \dots, D_n$ értékek közül egy "ellenségünk" birtokába kerül. Minden lehetséges D' értékre a $[0, p)$ halmazon pontosan egy olyan $q'(x)$ $k-1$ fokú polinom konstruálható úgy, hogy $q'(0) = D'$ és $q'(i) = D_i$ az összes $k-1$ titokrészre igaz. A konstrukcióból látszik, hogy minden lehetséges $q'(x)$ polinom azonos valószínűséggel fordulhat elő, tehát az "ellenségünk" nem kerül közelebb a D titok megfejtéséhez.

Egy ilyen (n, k) küszöbséma több hasznos tulajdonsággal rendelkezik:

(1) A titokrészek mérete nem haladja meg a titok méretét.

(2) Ha k fix, akkor egyes D_j titokrészek dinamikusan törölhetőek és hozzáadhatóak a sémához anélkül, hogy ez a többi D_i értéket befolyásolná.

(3) A D_i-k könnyen változtathatóak anélkül, hogy a D értéken változtatnánk, hiszen csak annyi a dolgunk, hogy egy másik $q(x)$ polinomot választunk. Az ilyen típusú gyakori változtatás nagyban javítja a biztonságot, mert a biztonsági réseket csak akkor lehet kihasználni, ha a megszerzett adatok ugyanabból a $q(x)$ polinomból származnak.

(4) A D_i értékek szétosztása során építhetünk hierarchikusabb sémát olyan módon, hogy bizonyos résztvevőknek több titokrészt adunk.

2.2. Blakley titokmegosztási sémája

Blakley sémája [3] geometriai jellegű. Sokban hasonlít Shamir sémájára, azonban polinom interpoláció helyett, hipersíkok és azok metszeteinek segítségével épül fel.

Válasszunk véletlenszerűen egy x pontot egy adott véges test fölötti t dimenziós vektortérben, a titok pedig legyen x első koordinátája. Ha az x pontot már kiválasztottuk, válasszunk az i-edik résztvevő számára egy a_i pontot a vektortérben. Az így kapott a_i pontoknak és az x koordinátáinak a segítségével, határozzuk meg a titokrészeket:

$$y_i = a_{1i}x_1 + a_{2i}x_2 + \cdots + a_{ti}x_t \ .$$

Az i-edik résztvevő által birtokolt titokrész az y_i, a különböző a_{ij} értékek pedig nyilvánosak. A titok rekonstrukciójához összegyűlt t darab résztevő rendelkezik egy-egy a fentihez hasonló egyenlőséggel. Az ezekből alkotott egyenlőség rendszernek, vagyis az

$$Ax = y$$

alakú lineáris egyenletnek az x a megoldása, a titok pedig x első koordinátája.

Minden titokrész egy számérték véges test fölött, a titok pedig egy vektor egy koordinátája ugyanezen test fölött. Ez azt jelenti, hogy Shamir sémájához hasonlóan, minden résztvevő pontosan akkora mennyiségű információt jegyez mint amekkora a titok. Azt azonban vegyük észre, hogy ez a séma nem tökéletes. Ahogy az összegyűjtött titokrészek száma növekszik, a lehetséges x pontok száma csökken, hiszen minden résztvevő tudja, hogy a keresett pont az ő hipersíkján helyezkedik el, $t-1$ résztvevő pedig már meg tud határozni egy olyan az egyenest, ami átmegy az x ponton.

3. fejezet

Gráfok bonyolultságának vizsgálati módszerei

Annak a meghatározása, hogy egy titokmegosztási sémában a résztvevőknek mennyi információt kell tárolniuk a titok méretéhez képest, mind elméleti, mind gyakorlati szempontból fontos kérdés. Dolgozatomban ezt a mérőszámot gráfokon vizsgálom. A fogalmak és a fejezetben használt gondolatmenet az [1]-ból származik.

Definíció 3.0.1 *Tegyük fel, hogy S titokmegosztási sémát, meghatározhatjuk egy G gráffal, ahol minden v csúcshoz tartozik egy ξ_v véletlen érték, a titok értéke pedig ξ és ezek azonos eloszlásúak. A séma* ***tökéletes*** *ha:*

(i) Ha v és w csúcs között vezet él G-ben akkor ξ_v és ξ_w együtt meghatározzák a ξ vagyis a titok értékét.

(ii) Ha A egy független élhalmaz, akkor ξ és $\{\xi_v : v \in A\}$ értékek együttese statisztikailag függetlenek.

Ahhoz, hogy az bonyolultságot pontosan definiálni tudjuk, szükségünk van az *entrópia* definíciójára [13], [19].

Definíció 3.0.2 *Egy η valószínűségi változó entrópiája:*

$$\boldsymbol{H}(\eta) := -p_1 \log_2(p_1) - \ldots - p_k \log_2(p_k),$$

ahol η a különböző k értékeket $p_1, \ldots, p_k$ valószínűséggel veszi fel.

A gráf egy v csúcsának a bonyolultsága lényegében azt méri, hogy a v-nek mennyi információt kell tárolnia a titok méretéhez képest. Ennek mérésére az entrópiát használjuk: $\mathbf{H}(\xi_v)/\mathbf{H}(\xi_s)$.

Egy adott gráf bonyolultsága pedig a legnagyobb bonyolultsággal rendelkező csúcs bonyolultságával egyenlő a legoptimálisabb tökéletes S sémában:

Definíció 3.0.3 *A G gráf bonyolultsága:*

$$C(G) = \inf_{S} \max_{v \in V} (\boldsymbol{H}(\xi_v)/\boldsymbol{H}(\xi_s)),$$

ahol az infimum az összes olyan S-re vonatkozik, ami G-t valósítja meg.

Általánosságban nem ismert, hogy egy tetszőleges gráfra az infimumot valamilyen elérési struktúra felveszi-e.

Egy másik, kevesebbet használt mérőszám az *átlagos bonyolultság*. Ennek definíciója a következő:

Definíció 3.0.4 *A G gráf átlagos bonyolultsága:*

$$\overline{C}(G) = \sum_{v \in V} \boldsymbol{H}(\xi_v)/\boldsymbol{H}(\xi_s)\,|V|.$$

Megjegyzés: A szakirodalom a bonyolultság (*complexity*) kifejezést csak az utóbbi időben kezdte el használni, a legtöbb korábbi cikkben a szerzők információs hányadosként (*information ratio*) hivatkoznak rá.

3.1. Alsó korlát

Az alsó korlát meghatározása gráfok esetében körülményes és összetett probléma. Összefüggő gráfok esetében azonban egyszerűen belátható, hogy $C(G)$ legalább 1. Ugyanis ha ξ_1 és ξ függetlenek, de ξ_1 és ξ_2 együttesen meghatározzák ξ-t, akkor ξ_2 legalább annyi (új) információt tartalmaz mint amennyit ξ.

Az előző gondolatmenetet *információelméleti módszernek* nevezzük, általánosabban megfogalmazva pedig a következőképpen írható le: ha a résztvevők P halmazának minden A részhalmazára kiszámítjuk az entrópiáját, akkor az így kapott $\{\mathbf{H}(A) : A \subseteq P\}$ összességre az entrópia tulajdonságai miatt teljesülnek a következők:

a) $\mathbf{H}(\emptyset) = 0$ és $\mathbf{H}(A) \geq 0$ minden más esetben

b) monotonitás: ha $A \subseteq B$ akkor $\mathbf{H}(A) \leq \mathbf{H}(B)$

c) szubadditivitás: $\mathbf{H}(A \cup B) + \mathbf{H}(A \cap B) \leq \mathbf{H}(A) + \mathbf{H}(B)$.

A titokmegosztás definíciójából további két tulajdonság következik:

d) erős monotonitás: ha A nem kvalifikált részhalmaz, B pedig kvalifikált és $A \subseteq B$, akkor
$\mathbf{H}(A) + \mathbf{H}(\xi) \leq \mathbf{H}(B)$

e) erős szubadditivitás: ha A és B kvalifikált részhalmazok, de $A \cap B$ nem az, akkor
$\mathbf{H}(A \cup B) + \mathbf{H}(A \cap B) + \mathbf{H}(\xi) \leq \mathbf{H}(A) + \mathbf{H}(B)$,

ahol $\mathbf{H}(\xi)$ a titok entrópiája/mérete.

Ezzel a technikával már precízen tudjuk igazolni, hogy a bonyolultság mindig legalább 1. Legyen a és b egy él két végpontja a G összefüggő, legalább két pontból álló gráfban. Ekkor a-ra és b-re felírhatjuk a c) tulajdonságot:

$$\mathbf{H}(ab) \leq \mathbf{H}(a) + \mathbf{H}(b).$$

Mivel ab kvalifikált, de b nem, a d) tulajdonság miatt $\mathbf{H}(b) + \mathbf{H}(\xi) \leq \mathbf{H}(ab)$. A két egyenlőtlenséget összeadva azt kapjuk, hogy $\mathbf{H}(\xi) \leq \mathbf{H}(a)$. Ez azt jelenti, hogy a-nak legalább annyi bitet kell megjegyeznie, mint amennyi a titokban van és ez igaz *minden lehetséges titokmegosztási rendszerben*. Tehát $C(G) \geq 1$.

Az *információelméleti módszer* lényege tehát, hogy egy adott G gráfra a fenti tulajdonságok segítségével belátjuk, hogy létezik olyan egyelemű részhalmaz amelyhez legalább $k \cdot \mathbf{H}(\xi)$ értéket rendelünk. Ebből következik, hogy ez a résztevő legalább a titok k-szorosát jegyzi meg, vagyis a G-n definiált titokmegosztási rendszerben $C(G) \geq k$.

Az egyenlőtlenségek linearitása miatt feltehető, hogy $\mathbf{H}(\xi) = 1$, így pedig az egyelemű halmazokon felvett értékek maximuma közvetlenül az alsó korlátot adja meg.

Az információelméleti módszeren kívül semmilyen más eljárás nem ismert, ami $C(G)$-re alsó korlátot adna, ezért a gráfok bonyolultságának alsó becslése során jelenleg csak ehhez tudunk folyamodni.

3.2. Felső korlát

Minden egyes konstrukció egy gráfon, vagy általában bármilyen elérési struktúrán felső korlátot ad a bonyolultságra. Például az 1.2.1 alapján a háromszög bonyolultsága legfeljebb 1. A három hosszúságú út bonyolultsága pedig az 1.2.2 szerint legfeljebb $1,5$.

Lemma 3.2.1 *A teljes páros gráf bonyolultsága legfeljebb* 1.

Bizonyítás. Legyen A és B a páros gráf két osztálya. A titok legyen egy s bit, r pedig egy véletlen bit. Ha A minden eleme r-t, B minden eleme pedig $r \oplus s$-t ismeri meg, akkor a titokmegosztás minden feltételnek megfelel és ilyen módon a bonyolultság 1. □

Lemma 3.2.2 *A teljes gráf bonyolultsága legfeljebb* 1.

Bizonyítás. Minden konstrukció felső korlátot határoz meg. Az n csúcsú teljes gráf $(2, n)$ küszöbsémát definiál, mert bármely 2 résztvevő közösen meg tudja fejteni a titkot. Shamir sémája pedig olyan konstrukció, ami küszöbsémákra 1 bonyolultságú titokmegosztást definiál, tehát $C(G) \leq 1$. □

A fenti állításokat használva tetszőleges G gráfra felső korlátot adhatunk meg. Ha G lefedhető teljes páros gráfokkal úgy, hogy minden csúcs legfeljebb k-ban van benne, akkor G bonyolultsága legfeljebb k. Annak alapján, hogy hogyan választjuk meg a teljes páros gráfokat, különböző korlátokat tudunk adni.

- Ha G-t élekkel fedjük le, az adódik, hogy $C(G) \leq n-1$, ahol n a csúcsok száma.
- Ha G-t csúcsokból induló csillagokkal fedjük le, akkor $C(G) \leq d+1$ adódik, ahol d a gráf maximális fokszáma.
- Ha G éleit megfelelően irányítjuk és az irányított csillagokat tekintjük, akkor $C(G) \leq (d+2)/2$ adódik.
- Stinson [6] igazolta, hogy $C(G) \leq (d+1)/2$.
- Erdős és Pyber [5] megmutatta, hogy minden gráf lefedhető teljes páros gráfokkal úgy, hogy minden csúcsot legfeljebb $c \cdot n/\log n$-szer fedünk le. Innen adódik, hogy $C(G) \leq c \cdot n/\log n$.

3.3. Gráfok meghatározott bonyolultsággal

A gráfok jelentős részére - a kis méretű csúcshalmazzal rendelkező gráfoktól, illetve néhány gráfcsaládtól eltekintve - a bonyolultság meghatározása általában megoldatlan probléma. A bonyolultságot sikerült meghatározni a maximum 5 [16], 6 [12], vagy 7 [14] csúccsal rendelkező gráfokra. A 9 csúcsú 8, vagy 9 élű gráfokkal a [15] foglalkozik. Az is ismert, hogy a teljes gráfok és teljes páros gráfok bonyolultsága 1, a háromnál hosszabb utak és az ötnél nagyobb körök bonyolultsága 3/2 [13]. [4]-ben sikerült találni egy végtelen gráfcsaládot $2-1/d$ bonyolultsággal, ahol d a maximális fokszám. Továbbá [11]-ben igazolták, hogy minden d egészhez létezik d-reguláris gráf $(d+1)/2$ bonyolultsággal. A [8] bizonyítja, hogy az d dimenziós kocka bonyolultsága $d/2$ és a d dimenziós rács bonyolultságát is meghatározza. A fák bonyolultsága pedig $2-1/c$, ahol c a legnagyobb mag elemszáma [9]. Az itt felsorolt gráfcsaládokkal a továbbiakban részletesen is foglalkozom.

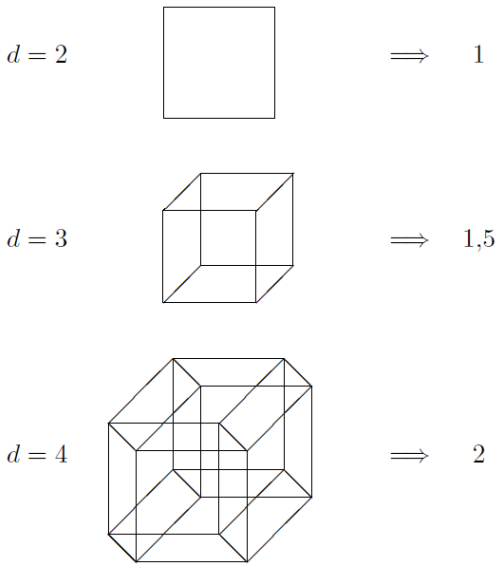
4. fejezet

Rekurzív módon felépíthető gráfok meghatározott bonyolultsággal

4.1. Titokmegosztás a d dimenziós kockán

Érdekes probléma a d dimenziós kocka (a továbbiakban K^d) bonyolultságának meghatározása, ezzel a [8] foglalkozik. Az alábbi bizonyítás is innen származik.

A négyzet teljes páros gráf, ezért 2 dimenziós esetben a pontos érték 1.



4.1.1 ábra [1]

A kocka részgráfként 3 hosszú utat tartalmaz. Az 1.2.2-ben megmutattuk, hogy a 3 hosszú út bonyolultsága legfeljebb $1,5$. Ismert, hogy ez a konstrukció optimális [1]. Mivel egy gráf bonyolultsága legalább annyi, mint részgráfjainak bonyolultsága, ezért a kocka bonyolultsága legalább $1,5$.

A felső korláthoz tehát $1,5$-ös bonyolultságú konstrukciót kell készítenünk. F véges test feletti két dimenziós T vektortérben legyenek $v_1, \ldots, v_6$ olyan vektorok, hogy bármelyik

kettő kifeszíti a teret. A vektorokat rendeljük a kocka lapjaihoz. A titok a vektortér egy s véletlen eleme. Ha $s \cdot v_1, \ldots, s \cdot v_6$ elemek közül kettőt ismerünk, abból az s kiszámolható. Az i-edik laphoz tartozó 4 csúcs között az $s \cdot v_i$ értéket úgy osztjuk el a négy csúcs között, hogy a két átellenes csúcsnak az F test egy véletlenszerűen kiválasztott r elemét adjuk, a maradék két csúcsnak pedig az $r + (s \cdot v_i)$ összeget. Minden csúcsot három lap tartalmazza, ezért a résztvevőknek az F test 3 elemét kell megjegyezniük. A titok pedig az F test fölötti 2 dimenziós tér egyik eleme, tehát ebben a konstrukcióban a bonyolultság $1,5$. Világos, hogy bármely két szomszédos csúcs meg tudja határozni az ahhoz a két laphoz tartozó skalárszorzatokat, amelyeken mindkét csúcs rajta van és így meg tudják fejteni a titkot. Az összes többi skalárszorzatról és így a titokról azonban nincs semmilyen információjuk.

Ahhoz, hogy az általános esetre is bizonyítsuk a tételt a 3 dimenziós esetben alkalmazott felső korlát konstrukciót kell módosítanunk úgy, hogy az d dimenziós esetben is működjön.

Tétel 4.1.1 *A $d \geq 2$ dimenziós kocka bonyolultsága $d/2$.*

Bizonyítás. Mivel egy tetszőleges élen a d dimenziós kocka $d-1$ darab két dimenziós hipersíkja osztozik, ezért az F test fölötti $d-1$ dimenziós vektortérből kell vektorokat választanunk a hipersíkokhoz. A csúcsok $\binom{d}{2}$ két dimenziós hipersík metszetében találhatóak, tehát a testnek ennyi elemét kell megjegyezniük. A titok pedig a test egy $d-1$ dimenziós vektora. A hányadosuk pedig: $\frac{\binom{d}{2}}{(d-1)} = d/2$.

Mielőtt az alsó korlát meghatározásával elkezdünk foglalkozni, vegyük észre, hogy a kockák esetében a bonyolultság és az átlagos bonyolultság megegyezik a K^d szimmetriáiból adódóan. Legyen H a K^d-t önmagába képező leképezések csoportja. H-nak $2^d \cdot d$ eleme van. Ha v és w (nem feltétlenül különböző) csúcsok K^d-ben, akkor az olyan π automorfizmusok száma, amelyekre teljesül, hogy $\pi(v) = w$ pontosan $|H| \,/\, \left|K^d\right| = d!$. Legyen ζ egy tökéletes titokmegosztási séma K^d-n, és alkalmazzuk ζ-t $\pi(K^d)$-re minden $\pi \in H$ estén. Az így kapott "összegsémában" a titok mérete $|H|$-szorosára nő és minden résztvevő $|H| \,/\, \left|K^d\right|$-szor annyi adatot jegyez meg, mint amennyi a ζ-ban megjegyezendő összes adat. Tehát az így kapott "összegsémában" minden résztvevő ugyanannyi adatot jegyez meg, ami azt jelenti, hogy a bonyolultság és átlagos bonyolultság egyenlő.

Legyen f az alábbi függvény egy gráf csúcshalmazán:

$$f(A) := \mathbf{H}(\{\xi_v : v \in A\})/\mathbf{H}(\xi).$$

Ekkor $\{f(v) : v \in V\}$ átlaga egyenlő az gráf átlagos bonyolultságával és definíciójából adódóan teljesülnek a 3.1 fejezetben megfogalmazott a)-e) tulajdonságok, hasonlóan mint $\mathbf{H}$-ra.

a) $f(\emptyset) = 0$ és $f(A) \geq 0$ minden más esetben

b) monotonitás: ha $A \subseteq B$, akkor $f(A) \leq f(B)$

c) szubadditivitás: $f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$

d) erős monotonitás: ha A nem kvalifikált részhalmaz, B pedig kvalifikált és $A \subseteq B$, akkor
$\mathbf{H}(A) + 1 \leq f(B)$

e) erős szubadditivitás: ha A és B kvalifikált részhalmazok de $A \cap B$ nem az, akkor
$f(A \cup B) + f(A \cap B) + 1 \leq f(A) + f(B)$

A fentiek következtében, a tétel bizonyításához elég belátnunk, hogy:

$$\sum \{f(v) : v \in V\} \geq d2^{d-1}.$$

Osszuk fel a d dimenziós kocka csúcshalmazát két egyenlő méretű A_d és B_d részre "sakktáblaszerűen", a szemközti csúcsokat azonos halmazba sorolva: $K^d = A_d \cup B_d$, ahol A_d és B_d függetlenek és $|A_d| = |B_d| = 2^{d-1}$. Az A_d-beli csúcsoknak csak B_d-ben vannak szomszédai és fordítva. A $(d+1)$ dimenziós kocka a d dimenziós kockának két független másolatát tartalmazza úgy, hogy azok csúcsai között teljes párosítás van. Ekkor K^{d+1} minden éle vagy a párosítás része, vagy a K^d egyik éle. Tegyük fel, hogy a két kisebb dimenziós kocka csúcsai el vannak osztva A_d-re és B_d-re, illetve A'_d-re és B'_d-re úgy, hogy A_d és B'_d, valamint A'_d és B_d között teljes párosítás van. K^{d+1} csúcsainak a felosztása történjen a következő módon:

$$A_{d+1} = A_d \cup A'_d \text{ és } B_{d+1} = B_d \cup B'_d.$$

Ennek a módszernek a segítségével használhatunk indukciót d-re. Az indukciós feltevés megfogalmazásához szükségünk lesz egy újabb definícióra:

$$[\![A, B]\!] := \sum_{b \in B} f(bA) - \sum_{a \in A} f(A - \{a\}).$$

A továbbiakban, amikor ezt a képletet használjuk, feltesszük, hogy A és B azonos elemszámúak.

Lemma 4.1.2 *A d dimenziós kockára $K^d = A_d \cup B_d$ felosztás mellett teljesül, hogy*

$$\sum_{v \in K^d} f(v) \geq [\![A_d, B_d]\!] + (d-1)2^{d-1}. \tag{4.1}$$

Bizonyítás. A $d = 1$ esetben igaz az állítás, hiszen az 1 dimenziós kocka egy a és egy b csúcsból áll, amelyek között 1 db él fut. Legyen $A_1 = \{a\}$ és $B_1 = \{b\}$. $d = 1$ esetben a (4.1) tehát:

$$f(a) + f(b) \geq f(ab) - f(\emptyset) + 0.$$

Ez az egyenlőtlenség pedig teljesül, mivel az f függvényre igaz a c) tulajdonság.

Tegyük fel, hogy a (4.1) teljesül a $d+1$ dimenziós kockában lévő két darab d dimenziós kockára, $A_{d+1} = A_d \cup A'_d$ és $B_{d+1} = B_d \cup B'_d$ felosztással. Az indukciós feltevés tehát így hangzik:

$$\sum_{v\in V_{d+1}} f(v) = \sum_{v\in V_d} f(v) + \sum_{v\in V_{d'}} f(v') \geq [\![A_d, B_d]\!] + [\![A'_d, B'_d]\!] + (d-1)2^d. \tag{4.2}$$

Minden $b \in B_d$ pontosan egy $a' \in A'_d$-vel van összekötve. Legyen (a', b) egy ilyen pár. Ekkor a c) tulajdonság miatt:

$$f(bA_d) - f(A_d) \geq f(bA_dA'_d - \{a'\}) - f(A_dA'_d - \{a'\}). \tag{4.3}$$

Az $a \in A_d$ legyen $b \in B_d$-hez kapcsolódó csúcs. Mivel b a-hoz és a'-höz is kapcsolódik bA'_d és $abA'_d - \{a'\}$ kvalifikált halmazok, metszetük $bA'_d - \{a'\}$ azonban független. Ez azt jelenti, hogy e)-ből adódóan:

$$f(bA'_d) - f(bA'_d - \{a'\}) \geq f(abA'_d) - f(abA'_d - \{a'\}) + 1.$$

Ezt az egyenlőtlenséget és a c) tulajdonságot kétszer felhasználva azt kapjuk, hogy

$$\begin{gathered} f(A'_d) - f(A'_d - \{a'\}) \geq f(bA'_d) - f(bA'_d - \{a'\}) \geq \\ \geq f(abA'_d) - f(abA'_d - \{a'\}) + 1 \geq f(bA_dA'_d) - f(bA_dA'_d - \{a'\}) + 1. \end{gathered}$$

Ezután ehhez az egyenlőtlenséghez hozzáadjuk a (4.3)-as egyenlőtlenséget, minden (a', b) $a' \in A'_d$ és $b \in B_d$ csúcspárra, akkor a következő egyenlőtlenséghez jutunk:

$$f(bA_d) - f(A_d) + f(A'_d) - f(A'_d - \{a'\}) \geq 1 + f(bA_dA'_d) - f(A_dA'_d - \{a'\}).$$

Ebben az egyenletben a kocka szimmetriái miatt (A_d, B_d) és (A'_d, B'_d) felcserélhetőek, tehát

$$f(b'A'_d) - f(A'_d) + f(A_d) - f(A_d - \{a\}) \geq 1 + f(b'A'_dA_d) - f(A'_dA_d - \{a\})$$

egyenlőtlenség is érvényes, minden (a, b') párra. Pontosan 2^{d-1} él fut A'_d és B_d között, továbá ugyanennyi él fut A_d és B'_d között is. Ha összeadjuk ezt a 2^d egyenlőtlenséget, a bal oldalon az $f(A_d)$-k és az $f(A'_d)$-k kiejtik egymást és a korábbi definíciókból az alábbi egyenlőtlenség következik:

$$[\![A_d, B_d]\!] + [\![A'_d, B'_d]\!] \geq [\![A_dA'_d, B'_dB_d]\!] + 2^d.$$

Vegyük észre, hogy ekkor a (4.2) segítségével a következőt kapjuk:

$$\sum_{v\in V_{d+1}} f(v) \geq [\![A_dA'_d, B'_dB_d]\!] + (d-1)2^d + 2^d.$$

Ez pedig pontosan az (4.1) egyenlőtlenség és mi ezt szerettük volna bebizonyítani. □

Ebből a 4.1.1-es tételt már egyszerűen be tudjuk látni. Legyen $K^d = A_d \cup B_d$ a csúcsok "sakktáblaszerű" felosztása. Mivel A_d-ben és B_d-ben is pontosan 2^{d-1} csúcs van, képesek vagyunk ezeket párosítani. Legyen (a, b) $a \in A_d$ és $b \in B_d$ egy ilyen pár. A d) tulajdonság miatt

$$f(bA_d) - f(A_d - \{a\}) \geq 1$$

hiszen $A_d - \{a\}$ nem kvalifikált, bA_d viszont igen. Ha vesszük az ilyen egyenlőtlenségek összegét minden (a, b) párra, akkor az alábbi egyenlőtlenséget kapjuk

$$[\![A_d, B_d]\!] = \sum_{b \in B_d} f(bA_d) - \sum_{a \in A_d} f(A_d - \{a\}) \geq 2^{d-1}.$$

Ez az egyenlőtlenség pedig a 4.1.2-es lemmával együtt a következő egyenlőtlenséget adja:

$$\sum_{v \in V_d} f(v) \geq (d-1)2^{d-1} + 2^{d-1} = d2^{d-1}.$$

Mivel a d dimenziós kockának 2^d csúcsa van, az átlagos bonyolultsága legalább $d/2$. Korábban már beláttuk, hogy a kocka esetében ez azt is jelenti, hogy a bonyolultság is legalább $d/2$, vagyis a bizonyítás teljes. □

Megjegyzés: Az d dimenziós *rács* olyan gráf, aminek csúcsait a d dimenziós tér pontjainak feleltethetjük meg, és két csúcs között akkor megy él, ha az általuk reprezentált pontok távolsága 1. A fentihez hasonló módszerrel sikerült bebizonyítani, hogy a $d \geq 2$ dimenziós rács bonyolultsága d [8].

4.2. $U_k^{n,p}$ és $S_k^{n,p}$ gráfcsaládok

A [11] foglalkozik azzal, hogyan tudunk bármilyen d egészre d-reguláris gráfot építeni, aminek bonyolultsága pontosan $(d+1)/2$.

Stinson a [6]-ban megmutatta, hogy ha a G gráf maximális fokszáma d:

$$C(G) \leq (d+1)/2.$$

A következőkben a [11] alapján, azt mutatom be, hogy lehet $U_k^{n,p}$ gráfot konstruálni $d = k+2$ maximális fokszámmal, np^{d-2} csúccsal, amire teljesül, hogy

$$(d+1)/2 \leq C(U_k^{n,p})$$

amennyiben $n, p \geq 6$ páros egész számok és $k \geq 0$ egész.

Lehetőségünk van még $U_k^{n,p}$ gráfosztály segítségével olyan $S_k^{n,p}$ gráfokat felépíteni, amelyeknek maximum foka $d = k+3$, $2np^{d-3}$ csúccsal rendelkeznek és teljesül, hogy

$$(d+1)/2 \leq C(S_k^{n,p}).$$

Definíció 4.2.1 *Ha n és p pozitív, páros, 6-nál nem kisebb egész számok, $k \geq 0$ pedig pozitív egész, akkor az $U_k^{n,p}$ gráfot a következő rekurzióval tudjuk felépíteni:*

1. *$U_0^{n,p} = (V(U_0^{n,p}), E(U_0^{n,p}))$ az n csúcsú kör, tehát*
   $V(U_0^{n,p} = \{v_0, \ldots, v_{n-1}\}$, $E(U_0^{n,p}) = \{(v_i, v_{i+1}) : 0 \leq i \leq n-2\} \cup \{(v_0, v_{n-1})\}$.

2. *Ha $k \geq 1$, legyen (R^{k-1}, L^{k-1}) az $U_{k-1}^{n,p}$ csúcshalmazának, vagyis $V(U_{k-1}^{n,p})$-nek a felosztása két egyforma méretű független csúcshalmazra:*

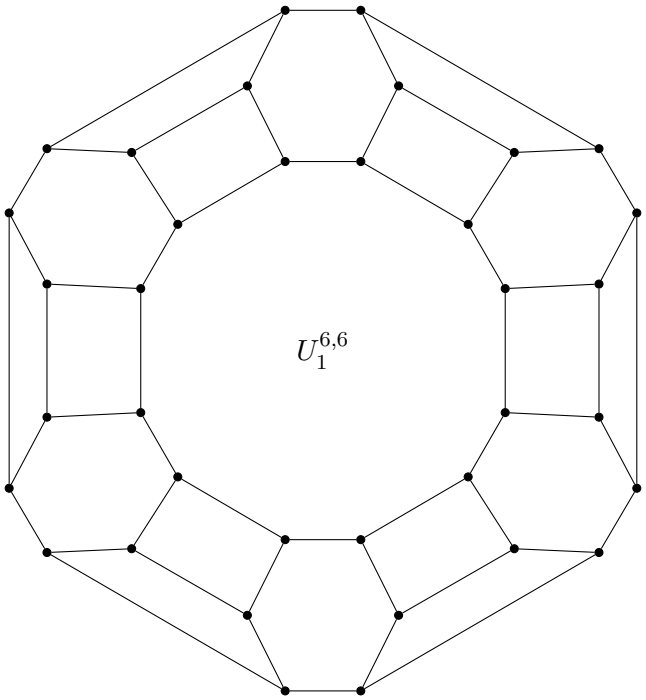
$$\left|R^{k-1}\right| = \left|L^{k-1}\right| = \left|V(U_{k-1}^{n,p})\right|/2 = np^{k-1}/2.$$

Vegyük az $U_{k-1}^{n,p}$ gráf p másolatát. Minden $a \in \{0,\dots,p-1\}$-hoz legyen R_a^{k-1} és L_a^{k-1} a két egyforma méretű független csúcshalmaza az $U_{k-1}^{n,p}$ a-adik másolatának. Az $U_k^{n,p}$ gráfot úgy kapjuk meg, hogy összekötjük az $U_{k-1}^{n,p}$ p másolatát úgy, hogy teljes párosítás legyen R_a^{k-1} és L_{a+1}^{k-1} csúcsai között, minden $a \in \{0,\dots,p-1\}$-re, ahol $a+1$-et modulo p vesszük.

A konstrukció jól definiált. Látható, hogy $k=0$ esetben az $U_k^{n,p}$ gráf egy n csúcsú kör, amely könnyen szétoszthatóra két független $n/2$ elemszámú részhalmazra. Ha $k \geq 1$, a két független $np^k/2$ elemszámú csúcshalmaza $U_k^{n,p}$-nak:

$$L^k = \bigcup_{a=0}^{p-1} L_a^{k-1} \text{ és } R^k = \bigcup_{a=0}^{p-1} R_a^{k-1}.$$

Nem nehéz belátni, hogy az $U_k^{n,p}$ $k+2$-reguláris gráf. A $k=1$ esetre, az $U_k^{6,6}$ gráf a 4.2.1 ábrán látható.



4.2.1 ábra

A [11] definiál egy másik, $S_k^{n,p}$-val jelölt gráfcsoportot is, $d = k+3$ maximum fokszámmal, amire teljesül, hogy

$$(d+1)/2 \leq C(S_k^{n,p}),$$

azonban csak $2np^d - 3$ csúcsa van.

Legyenek $\left\{v_1,\dots,v_{np^k}\right\}$ az $U_k^{n,p}$ gráf csúcsai. Az $S_k^{n,p}$ gráfot az $U_k^{n,p}$ gráfból úgy kapjuk, hogy $U_k^{n,p}$-t kiegészítjük $\left\{w_1,\dots,w_{np^k}\right\}$ új csúcsokkal, és (v_i,w_i) új élekkel, minden $i = 1,\dots,np^k$-ra.

5. fejezet

Titokmegosztás fákon

A fákkal leírható elérési struktúrák bonyolultsága pontosan $2 - 1/c$, ahol c a fa legnagyobb magjának az elemszáma. A gráf csúcsainak egy részhalmaza akkor alkot magot, ha összefüggő, továbbá minden csúcsnak ebben a részhalmazban van a részhalmazon kívüli, a részhalmaz többi tagjától és egymástól független szomszédja. Az állítás és az alábbi bizonyítása [9]-ból származik.

Definíció 5.0.2 *Egy G gráf csúcsainak X részhalmazát G magjának nevezzük, ha összefüggő és minden $x \in X$-nek van $x' \notin X$ szomszédja úgy, hogy x' egyetlen X-beli szomszédja x, továbbá $\{x' | x \in X\}$ független csúcshalmaz a gráfban.*

Definíció 5.0.3 *Legyen $G = (V, E)$, $G_i = (V_i, E_i)$ $(i = 1, \ldots, m)$ pedig G részgráfjai. $\{G_i\}$ fedése G-nek, ha $V \subseteq \bigcup V_i$.*

A részgráfokhoz súlyokat is rendelhetünk. Ebben az esetben egy csúcs vagy él súlya a fedésben egyenlő a csúcsot vagy élt tartalmazó részgráfok összsúlyával. Ha a súlyok nem feltétlenül pozitív egészek, akkor *tört fedés*ről beszélünk. Amennyiben minden G_i csillag, akkor azt csillagfedésnek nevezzük.

Definíció 5.0.4 *Egy G gráf csillagfedés rátája a maximális csúcs súlyok infimuma az összes lehetséges tört csillagfedés között, ahol minden élt legalább egyszer fedünk le.*

Fák esetében a csúcsok egy X részhalmaza akkor alkot magot, ha X elemei összefüggőek és mindnek van szomszédja X-en kívül.

Tétel 5.0.5 *Tetszőleges G gráfra, $c = c(G)$ legyen a G egy maximális méretű magjának elemszáma, $s = s(G)$ pedig G csillagfedés rátája. Ekkor $2 - 1/c \leq C(G) \leq s$.*

Bizonyítás. A tételben lévő a $C(G) \leq s$ egyenlőtlenséget a [6]-ban Stinson bizonyította. A másik egyenlőtlenség bizonyítását az információelméleti módszer segítségével fogjuk elvégezni. A 4.1 fejezetben definiáltuk az

$$f(A) := \mathbf{H}(\{\xi_v : v \in A\})/\mathbf{H}(\xi)$$

függvényt a gráf csúcshalmazán. Most is ezt az f-et fogjuk használni és az a)-e) tulajdonságok továbbra is teljesülnek.

Az 5.0.5-ös tétel első egyenlőtlenségének bizonyításához szükségünk van az alábbi lemmára.

Lemma 5.0.6 *Ha X a G gráf magja, f pedig a fent definiált függvény, és teljesülnek rá az a)-e) tulajdonságok, akkor*

$$\sum_{\{v\}\in X} f(v) \geq 2\,|X| - 1$$

Bizonyítás. $|X| \leq 1$ esetén az állítás triviális. Tehát elég a $|X| \geq 2$ esetekkel foglalkoznunk. A bizonyításhoz a "független szekvencia lemmát" fogjuk használni [7], [10]:

Lemma 5.0.7 *Tegyük fel, hogy $A = \{v_1, \ldots, v_n\}$ összefüggő és létezik $B = \{w_1, \ldots, w_n\}$ független halmaz úgy, hogy minden w_i pontosan egy v_i-vel van összekötve. Ekkor $f(A) \geq |A| + 1$.*

Bizonyítás. Vizsgáljuk a következő d_i különbségeket:

$$d_i := f(Aw_1 \ldots w_i) - f(w_1 \ldots w_i).$$

Mivel $f(\emptyset) = 0$, d_0-t szeretnénk megkapni. Vegyük sorba a d_i számokat fordított sorrendben. Nyilvánvalóan AB kvalifikált részhalmaz, B pedig nem az, ezért alkalmazhatjuk az f függvény d) tulajdonságát, amiből azt kapjuk, hogy $f(AB) - f(B) \geq 1$ ($d_n \geq 1$).

Belátjuk, hogy minden $1 \leq i \leq n$ esetén $d_i + 1 \leq d_{i-1}$. Ebből pedig következik, hogy $d_0 \geq n + 1$, ahogy azt a lemma kimondja.

Tudjuk, hogy $v_i w_1 \ldots w_i$ és $Aw_1 \ldots w_{i-1}$ kvalifikáltak, $v_i w_1 \ldots w_{i-1}$ (vagyis a metszetük) azonban nem az. Az f függvény erős szubadditivitása miatt:

$$f(v_i w_1 \ldots w_i) + f(Aw_1 \ldots w_{i-1}) \geq f(v_i w_1 \ldots w_{i-1}) + f(Aw_1 \ldots w_i) + 1.$$

A szubadditivitásból következik:

$$f(w_1 \ldots w_i) + f(v_i w_1 \ldots w_{i-1}) \geq f(w_1 \ldots w_{i-1}) + f(v_i w_1 \ldots w_i).$$

A két egyenlőtlenséget összeadva és átrendezve megkapjuk, hogy $d_i + 1 \leq d_{i-1}$. Tehát a "független szekvencia lemmát" beláttuk. □

Az X mag, ezért nyilvánvalóan teljesül rá a 5.0.7-es lemma, vagyis:

$$f(X) \geq |X| + 1$$

Ennek az egyenlőtlenségnek a használatával elég belátnunk, hogy:

$$\sum_{\{v\}\in X} f(v) \geq f(X) + |X| - 2. \tag{5.1}$$

Ezt az egyenlőtlenséget minden X összefüggő részhalmazra be tudjuk látni, nem csak magokra. Ha $X = \{v, w\}$, tehát X csak két csúcsból áll, akkor az (5.1)-es egyenlőtlenséget X-re felírva:

$$f(\{v\}) + f(\{w\}) \geq f(\{v, w\}),$$

ez az egyenlőtlenség pedig az f függvény c) és e) tulajdonságai miatt teljesül.

Tegyül fel, hogy X tartalmaz három, vagy több csúcsúból álló összefüggő részgráfot. Válasszunk egy $v \in X$ csúcsot úgy, hogy $Y = X - \{v\}$ összefüggő legyen (ilyen v csúcs mindig létezik). Legyen $w \in Y$ olyan csúcs, hogy v és w összefüggő. Ekkor Y és $\{v, w\}$ is összefüggő, de a metszetük $\{w\}$ független, vagyis az f függvény e) tulajdonságát felhasználva:

$$f(\{v, w\}) + f(Y) \geq f(X) + f(\{w\}) + 1.$$

Korábban már láttuk, hogy c) tulajdonság szerint:

$$f(\{v\}) + f(\{w\}) \geq f(\{v, w\}).$$

Ha ezt a két egyenlőtlenséget összeadjuk, azt kapjuk, hogy:

$$f(\{v\}) + f(Y) \geq f(X) + 1.$$

Ha pedig ezt az egyenlőtlenséget és az indukciós feltevést Y-ra összeadjuk, megkapjuk az (5.1) egyenlőtlenséget, tehát a lemmát bebizonyítottuk. □

A ha az 5.0.6-os lemmát a legnagyobb (c elemszámú) magra alkalmazzuk, majd az egyenlőtlenséget osztjuk c-vel, pontosan az 5.0.5-ös tétel első egyenlőtlenségét kapjuk. □

Tétel 5.0.8 *Tetszőleges G fára ha $c = c(G)$ a G egy maximális méretű magjának elemszáma, $s = s(G)$ pedig G csillagfedés rátája teljesül, hogy $2 - 1/c = C(G) = s$.*

Ez a tétel következik az 5.0.5-ös tételből, illetve az alábbi lemmából.

Lemma 5.0.9 *Ha G egy legalább 2 csúcsúból álló fa és G maximális magjának mérete nem nagyobb mint c, akkor létezik olyan csillagfedése G-nek, hogy az*

(i) minden élt pontosan c-szer fed le,

(ii) minden csúcsot maximum $2c - 1$-szer fed le.

Bizonyítás. Cseréljünk ki minden irányítatlan (u, v) élt G-ben c darab irányított élre u és v között. Az egyes élek irányát később adjuk meg.

A csillagfedés elkészítéséhez a már irányított élek segítségével határozzuk meg a csillagokat olyan módon, hogy minden él a csillag középpontjától kifelé irányul. Tehát minden v-ből kimenő él egy v középpontú csillag része. Ilyen módon annyi v középpontú csillagot készíthetünk, amennyi a maximális kimenő élek száma v-ből. Továbbá v pontosan annyi csillagnak lesz szélső csúcsa, amennyi a bejövő élek száma v-be. Ennek a két számnak az összege egyenlő a v-t fedő csillagok számával. Mivel pontosan c irányított él van minden eredeti él helyén, ez a szám c plusz az összes bejövő irányított élek száma, kivéve a bejövő élek számát abból a szomszédból, ahonnan a legkevesebb bejövő él érkezik.

Tehát az kell igazolnunk, hogy lehetséges az éleket úgy irányítani, hogy az összeg második tagja legfeljebb $c-1$.

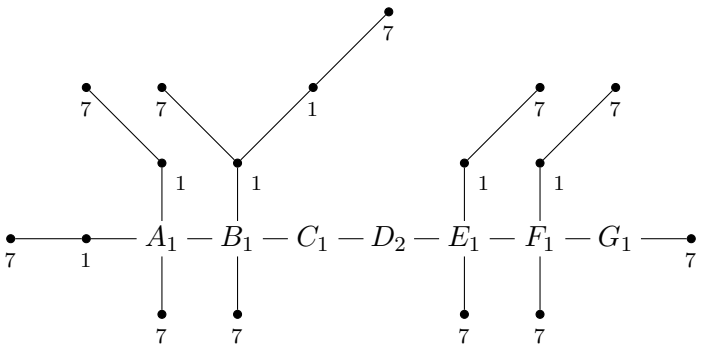
Kezdjük el a csúcsokat pozitív egész számokkal súlyozni. Egy csúcshalmaz súlya legyen egyenlő a halmazban lévő csúcsok súlyának összegével. A súlyozás segítségével biztosítani fogjuk, hogy minden csúcs egy maximális súlyú magban legyen.

Legyen $\mathcal{W}$ az olyan pozitív egész súlyfüggvények halmaza, amelyek szerint minden mag súlya maximum c. Mivel minden csúcs eleme valamilyen magnak, és $\mathcal{W}$ véges elemszámú. Továbbá $\mathcal{W}$ nem üres, hiszen ha minden csúcs súlya 1, akkor c definíciója szerint minden mag súlya $\leq c$. Akkor mondjuk egy $w \in \mathcal{W}$ súlyfüggvényre, hogy *maximális*, ha a súlyfüggvény amit úgy kapunk, hogy w-t 1-el növeljük bármely csúcsán, már nem eleme $\mathcal{W}$-nek. Nyilvánvalóan létezik maximális súlyfüggvény $\mathcal{W}$-ben.

Legyen $w \in \mathcal{W}$ maximális súlyfüggvény. Ekkor w maximalitásából következik, hogy minden v csúcshoz létezik olyan mag, ami v-t tartalmazza és pontosan c súlyú.

Legyen (v_1, v_2) egy él G-ben. Ha v_1 vagy v_2 levél, akkor irányítsuk mind a c élt v_1 és v_2 között a levél irányába (ha v_1 és v_2 is levél, akkor G egy élből áll, és ebben az esetben teljesül a tétel, akárhogy irányítjuk az éleket).

Ha v_1 sem és v_2 sem levél, akkor a (v_1, v_2) él eltávolításával két független fára bontjuk szét a gráfot. Legyenek ezeket a fák G_1 és G_2, ahol G_i tartalmazza a v_i csúcsot. Legyen C_i a maximális súlyú mag (w súlyfüggvény szerint) G_i-ben ami tartalmazza v_i-t, és legyen a súlya $c_i = w(C_i)$. Mivel $C_1 \cup C_2$ egy $c_1 + c_2$ súlyú mag G-ben és G minden magjának súlya $\leq c$, ezért $c_1 + c_2 \leq c$. Irányítsuk a c irányított élt v_1 és v_2 között úgy, hogy közülük c_1 mutasson v_1-ből v_2-be, és c_2 pedig v_2-ből v_1-be.



5.0.1. ábra

Az 5.0.1. ábrán látható fa maximális magjának mérete $c = 7$. A számok a maximális súlyfüggvényt mutatják. Minden él helyére 7 irányított él kerül. Ha a fenti eljárás segítségével irányítjuk őket, a következő számokhoz jutunk:

$$A \underset{3}{\longrightarrow} B \; B \underset{6}{\longrightarrow} C \; C \underset{\geq 1}{\longrightarrow} D \; D \underset{2}{\longrightarrow} E \; E \underset{4}{\longrightarrow} F \; F \underset{6}{\longrightarrow} G$$

$$A \underset{4}{\longleftarrow} B \; B \underset{1}{\longleftarrow} C \; C \underset{\geq 2}{\longleftarrow} D \; D \underset{5}{\longleftarrow} E \; E \underset{3}{\longleftarrow} F \; F \underset{1}{\longleftarrow} G$$

Például, amikor a CD élt kitöröljük, az egyetlen mag a kapott gráfban ami D-t tartalmazza az egyelemű $\{D\}$, súlya pedig 2. Ezért $C \leftarrow D$-hez rendelt érték ≥ 2 és hasonlóan a $C \rightarrow D$-hez rendelt érték ≥ 1. Ez azt jelenti, hogy marad 4 él C és D között, amit szabadon irányíthatunk. Minden más élre a példában teljesül, hogy $c_1 + c_2 = c$, tehát minden más él iránya meghatározott.

Abban az esetben, ha v levél, c bejövő éle van és 0 kimenő éle. Ha pedig v nem-levél, akkor legyen C maximális súlyú mag w szerint, ami tartalmazza v-t. Feltettük, hogy w maximális, ezért C súlya c. Ha kitöröljük v-t C-ből, az így kapott gráf minden komponense v-nek pontosan egy szomszédját tartalmazza. Legyenek $v_1, v_2, \ldots v_s$ ezek a szomszédok és $C_1, C_2, \ldots C_s$ pedig a $C - v$ komponensei úgy, hogy C_i tartalmazza v_i-t. Ekkor

$$c = w(C) = w(v) + w(C_1) + w(C_2) + \cdots + w(C_s).$$

C és $C - C_i$ magok $G - vv_i$-ben és figyelembe vettük őket, amikor a vv_i éleket irányítottuk. Ez azt jelenti, hogy legalább $w(C_i)$ élt irányítottunk v_i-ből v-be és legalább $w(C - C_i)$ élt irányítottunk v-ből v_i-be. Így minden élt irányítottunk v és v_i között. Tehát a v-be bejövő élek összege C-beli csúcsokból

$$w(C_1) + w(C_2) + \cdots + w(C_s) = c - w(v) \leq c - 1.$$

Két eset lehetséges: v-nek van levél szomszédja, vagy nincs. Az első esetben, v minden nem-levél szomszédja C-ben található, mivel C-t maximálisnak választottuk. Nincsenek bejövő élek levelekből, tehát ebben az esetben kész vagyunk.

A második esetben v egyetlen szomszédja sem levél. Ebben az esetben is a maximalitás miatt v minden szomszédja C-ben van, kivéve egy v^* szomszédot. $C - C_i$ mag a $G - vv^*$ gráfban és tartalmazza v-t, tehát legalább $w(C - C_i) = c - w(C_i)$ élt irányítottunk v-ből v^*-ba. Ez azt jelenti, hogy a v^*-ből bejövő élek száma nem lehet több mint $w(C_i)$, ami a pedig a bejövő élek száma v_i-ből. Tehát megmutattuk, hogy a legkevesebb bejövő él v^*-ból jön és az összes bejövő élek száma más szomszédokból legfeljebb $c - 1$. □

6. fejezet

$2 - 1/d$ bonyolultsággal rendelkező gráfok családja

Tétel 6.0.10 *Legyen G egy d maximális fokszámmal rendelkező gráf, amire teljesülnek a következő tulajdonságok:*

(A) minden csúcsnak legfeljebb egy szomszédja van, amelynek fokszáma 1;

(B) azok a csúcsok, amelyeknek fokszáma legalább 3 nem szomszédosak;

(C) nem szerepel benne 6-nál kevesebb csúcsúból álló kör részgráfként.

Ekkor

$$C(G) = 2 - 1/d.$$

Ez a tétel és a hozzá tartozó bizonyítás [4]-ből származik.

6.1. Alsó korlát

Az alsó korlát meghatározásához ismét az információelméleti módszerhez folyamodunk. Legyen f a 4.1. és 5. fejezetben is alkalmazott függvény, amelyre teljesülnek az a)-e) tulajdonságok.

Állítás 6.1.1 *Tegyük fel, hogy G gráfnak létezik összefüggő A részgráfja, amire teljesül, hogy van olyan B részhalmaz G csúcsai között, hogy minden A-beli csúcsnak pontosan 1 szomszédja van a B-ben és minden A-beli csúcs különböző B-beli csúccsal szomszédos. Ekkor G bonyolultsága legalább $2 - 1/|A|$.*

Bizonyítás. A fák bonyolultságáról szóló korábbi fejezetben beláttuk, hogy egy gráf G minden X összefüggő csúcshalmazára:

$$\sum_{\{v\} \in X} f(v) \geq f(X) + |X| - 2. \tag{6.1}$$

Továbbá kimondtuk és bebizonyítottuk a "független szekvencia lemma"-t [7], [10]:

Lemma 6.1.2 *Tegyük fel, hogy $A = \{v_1, \ldots, v_n\}$ összefüggő és létezik $B = \{w_1, \ldots, w_n\}$ független halmaz úgy, hogy minden w_i pontosan egy v_i-vel van összekötve. Ekkor $f(A) \geq |A| + 1$.*

A feltételek a 6.1.1-es állítás feltevése és a lemma feltevése ugyanaz, tehát alkalmazhatjuk a lemmát. Adjuk össze lemmában szereplő egyenlőtlenséget a (6.1)-es egyenlőtlenséggel.

$$\sum_{\{v\} \in A} f(v) \geq 2\,|A| - 1. \tag{6.2}$$

Ebből következik, hogy van legalább egy olyan $v \in A$ csúcs amire $f(v) \geq 2 - 1/\,|A|$, vagyis a 6.1.1-es állítást bebizonyítottuk. □

Legyen G olyan gráf, amire teljesülnek az 6.0.10-es tételben meghatározott tulajdonságok. Feltételezhetjük, hogy $d \geq 2$, hiszen egyébként $C(G) \geq 1$ triviálisan teljesül. Legyen v_1 egy d fokszámú csúcs G-ben és legyen A olyan halmaz, ami egy kivételével v_1 összes szomszédját tartalmazza. Az A-nak pontosan d eleme van, legyenek ezek az elemek $v_1, v_2, \ldots v_d$. Nyilvánvaló, hogy A összefüggő. Legyen $v_i \in A$ bármelyik olyan csúcs A-ban, amire $i > 1$. Ez a v_i csúcs egy út része G két csúcsa között, tehát van még egy w_i szomszédja. Legyen w_1 a v_1 csúcs azon szomszédja, amelyik nem szerepel A-ban. Az így kapott $A = \{v_1, \ldots, v_d\}$ és $B = \{w_1, \ldots, w_d\}$ teljesítik a 6.1.1-es állítás feltételeit. Tehát megkaptuk az alsó korlátot a 6.0.10-es tételhez, vagyis beláttuk, hogy $C(G) \geq 2 - 1/d$.

6.2. Felső korlát

Készíteni fogunk egy olyan csillagfedést egy tetszőleges G-hez, ami teljesíti a 6.0.10-es tétel (A), (B), (C) tulajdonságait. Ebben minden élt d csillaggal és minden csúcsot maximum $2d-1$ csillaggal fedünk le, ezzel pedig Stinson eredményeinek [6] következményeként megkapjuk a felső korlátot, amire szükségünk van a tétel bizonyításához.
A csillagfedés két fő részből áll:

i) $d - 1$ darab u középpontú csillag minden $u \in V$ csúcsra aminek fokszáma ≥ 3.

A csillagfedés másik főbb része a gráf legalább 3 fokszámú csúcsait összekötő utakon lévő éleket fogja lefedni. Nyilvánvalóan egy fedő csillag lehet egyetlen él, vagy egy 2 élből álló út. Legyenek u és v legalább 3 fokszámú csúcsok és $u = v_0, v_1, \ldots, v_t = v$ egy G-beli út csúcsai u és v között. A fedés különböző lesz, eltérő paritású úthosszúságok esetén. Páratlan esetben, vagyis ha $t = 2k + 1$:

ii) 1 darab $v_{i-1} - v_i - v_{i+1}$ csillag, minden $i = 1, 3, \ldots, 2k - 1$ és $i = 2k$ esetén

iii) $d - 1$ darab $v_{i-1} - v_i - v_{i+1}$ csillag, minden $i = 2, 4, \ldots, 2k - 2$

iv) $d - 2$ darab $\{v_{2k-1}, v_{2k}\}$ él.

Ha az út hossza páros, akkor elhagyhatjuk a $v_{2k-1} - v_{2k} - v_{2k+1}$ csillagot az ii)-ból és az éleket az iv)-ből.

Látható, hogy minden élt pontosan d csillaggal fedtünk, minden út első és utolsó két csúcsát $2d-1$-szer fedtük le, az utak fennmaradó, belső csúcsait pedig legfeljebb $2d-1$-szer. Ezzel a 6.0.10-es tételt beláttuk.

7. fejezet

Kis gráfok bonyolultsága

7.1. Alsó korlát meghatározása lineáris programozás segítségével

A [17] foglalkozik azzal, hogyan kereshetünk alsó korlátot lineáris programozás segítségével. Ha felírjuk az információelméleti módszer leírásában bemutatott a)-e) egyenlőtlenségeket a csúcsok minden részhalmazára minden lehetséges módon, megkapjuk az LP feladat korlátozó egyenlőtlenségeit. A célfüggvényben pedig az egyelemű részhalmazok által megjegyzett maximumot kell minimalizálnunk. Az ilyen módon definiált LP-ben, az ismeretlenek és az egyenelőtlenségek száma nagy csúcsszám esetén túl nagy ahhoz, hogy a módszert nagy gráfokra alkalmazhassuk.

7.2. Csillagfedés keresése lineáris programozási feladatként

Egy adott $G(V, E)$ gráfhoz kereshetünk csillagfedést lineáris egyenlőtlenségek segítségével [4], amelyekre teljesülnek a következő tulajdonságok:

- minden $uv \in E$ élt lefedünk pontosan $e \in \mathbb{N}$ darab csillaggal,
- minden $v \in V$ csúcsot lefedünk legfeljebb $p \in \mathbb{N}$ csillaggal,
- a p/e érték minimális.

Tört csillagfedés esetén feltehetjük, hogy $e = 1$ és $p \in \mathbb{Q}$.

A lineáris programozási feladat változói:

- p: legtöbbször lefedett csúcsot fedő csillagok száma,
- x_{uv}, x_{vu} minden $uv \in E$ élre: az uv élt fedő u és v középpontú csillagok száma,
- l_u minden $u \in V$ csúcsra: az u középpontú csillagok száma.

Az LP feladat tehát háromféle egyenlőtlenségből áll:

- $x_{uv} + x_{vu} \geq 1$ minden élre,
- $l_u + \sum_{uv \in E} x_{uv} \leq p$ minden csúcsra,
- $x_{uv} \leq l_u$ minden csúcsra és élre,

ahol p értékét szeretnénk minimalizálni.

Látható, hogy az LP feladat $2|E| + |V| + 1$ változóból és $3|E| + |V|$ egyenletből áll, vagyis bármilyen LP problémákat kezelő szoftver segítségével néhány másodperc alatt megoldható, még nagy csúcs- és élszámú gráfok esetében is.

Fontos megjegyezni, hogy a csillagfedés sok esetben - például az 5-nél rövidebb köröket tartalmazó gráfok esetén - nem ad optimális becslést a bonyolultságra.

7.3. Eredmények

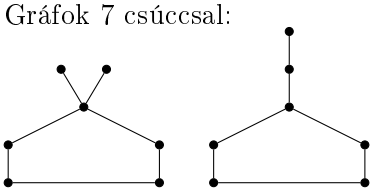
A 7.1 és 7.2 alfejezetekben tárgyalt LP feladatok alkalmazása során a következő problémákba ütközhetünk. Az alsó korlát megkeresésre szolgáló LP feladatot nagy csúcsszám esetén nem lehet egy átlagos teljesítményű számítógépen elég gyorsan lefuttatni ahhoz, hogy érdemben tudjuk vizsgálódni (10 csúcs esetén már 2^{10} változóból közel 2 millió egyenlőtlenségből álló rendszert kell megoldanunk). A csillagfedés pedig nem minden esetben ad optimális felső korlátot (például, ha a gráfban van 5-nél kisebb kör).
A két LP feladatot összesen 117 kis méretű gráfon futtattam le:

- 7 csúcsú, 7-nél nagyobb élszámú és 5-nél kisebb kört nem tartalmazó,
- 8 csúcsú, 8-nál nagyobb élszámú és 5-nél kisebb kört nem tartalmazó,
- 9 csúcsú, 9, 10, vagy 11 élszámú, 5-nél kisebb kört tartalmazó gráfokon.

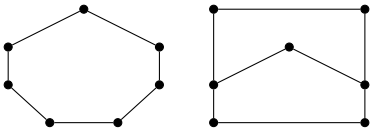
Ezekben az esetekben kivétel nélkül teljesült az alsó és felső korlát azonossága.

A vizsgált gráfok egy része a [4]-ben bemutatott gráfcsalád tagja. Továbbá az itt felsorolt 7 csúcsú gráfok bonyolultságáról [14]-ben, valamint [18]-ban írtak. A 9 csúcsú, 8 vagy 9 élű gráfok bonyolultságával pedig [15]-ben foglalkoztak, azonban a szerzők által leírt eredmények több esetben, pontatlanok és ellentmondanak a [4]-nek, a [9]-nek és az ebben, valamint a 8. fejezetben megfogalmazott eredményeknek is.

Gráfok 7 csúccsal:

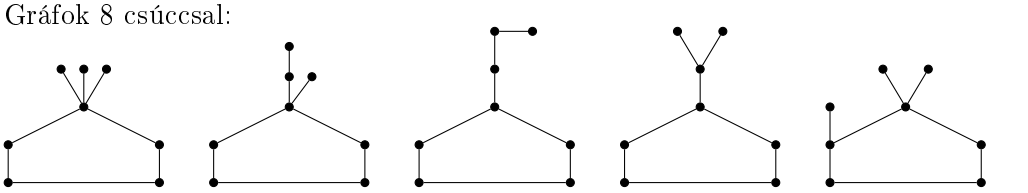


1 2 3 4 5

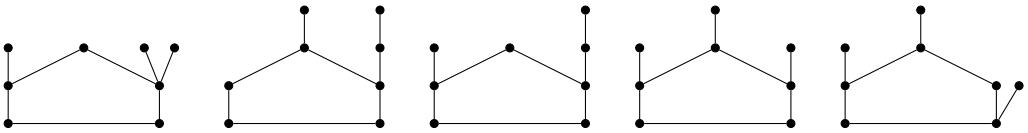


6 7

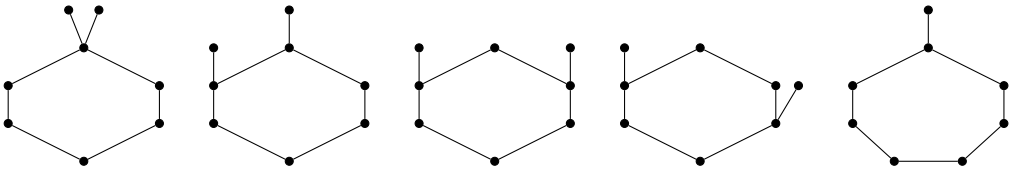
Gráfok 8 csúccsal:



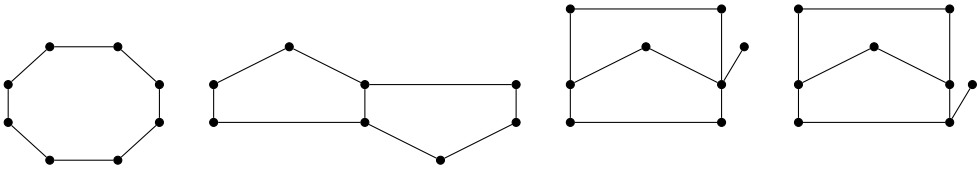
8 9 10 11 12



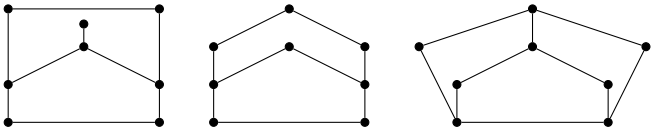
13 14 15 16 17



18 19 20 21 22

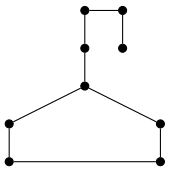


23 24 25 26

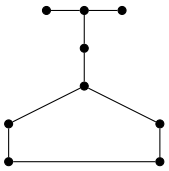


27 28 29

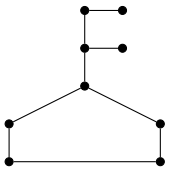
Gráfok 9 csúccsal és 9 éllel:



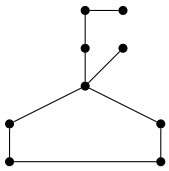
30



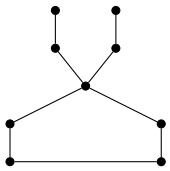
31



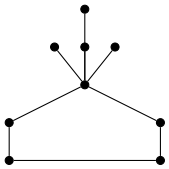
32



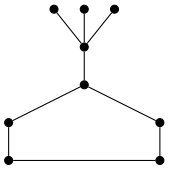
33



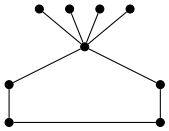
34



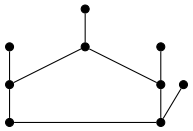
35



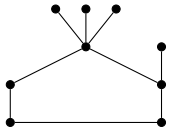
36



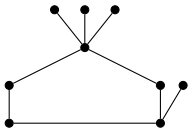
37



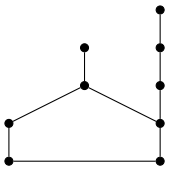
38



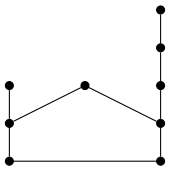
39



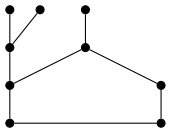
40



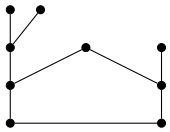
41



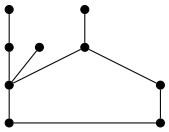
42



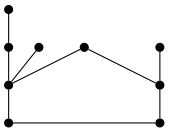
43



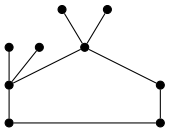
44



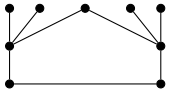
45



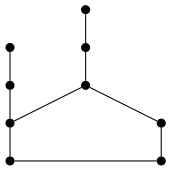
46



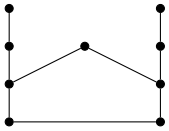
47



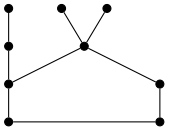
48



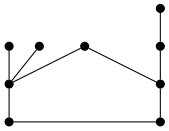
49



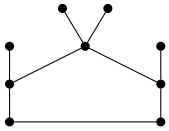
50



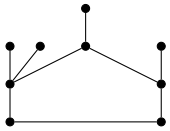
51



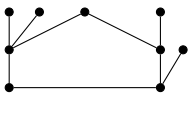
52



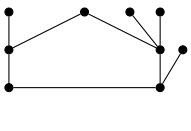
53



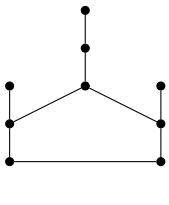
54



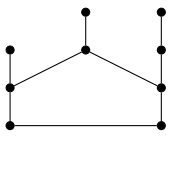
55



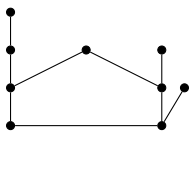
56



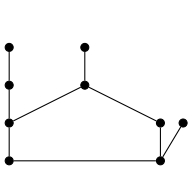
57



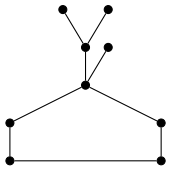
58



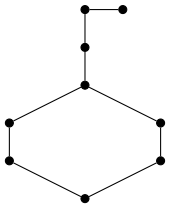
59



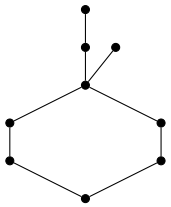
60



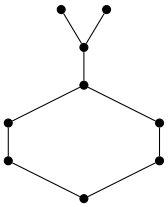
61



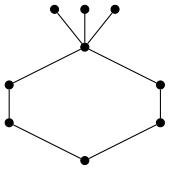
62



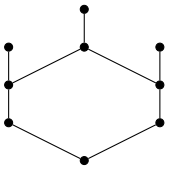
63



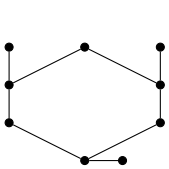
64



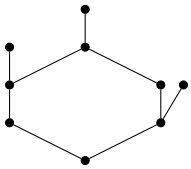
65



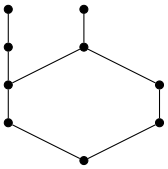
66



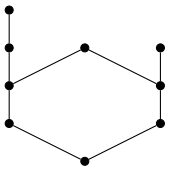
67



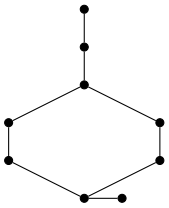
68



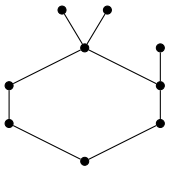
69



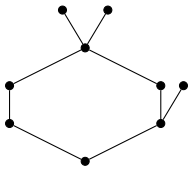
70



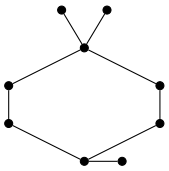
71



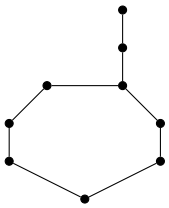
72



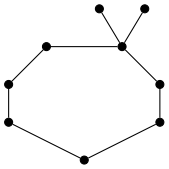
73



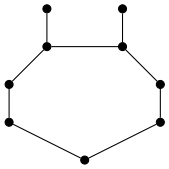
74



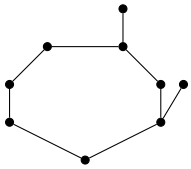
75



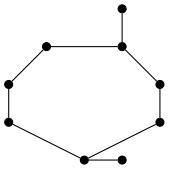
76



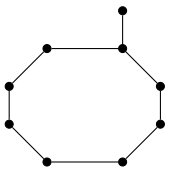
77



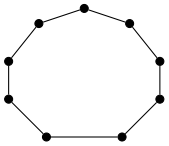
78



79

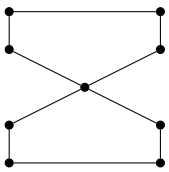


80

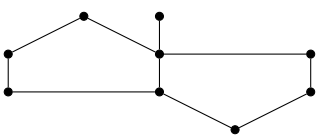


81

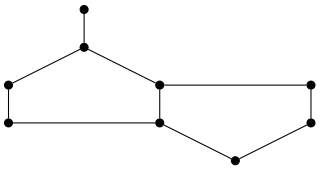
Gráfok 9 csúccsal és 10 éllel:



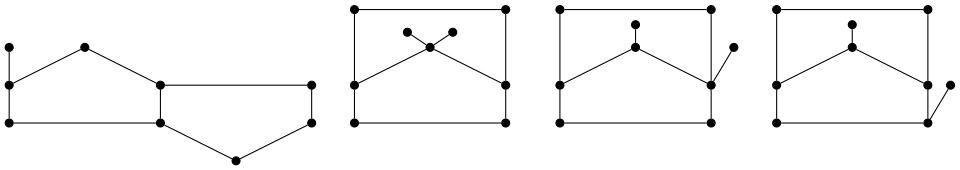
82



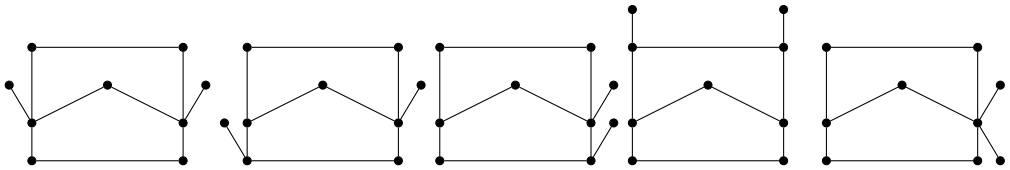
83



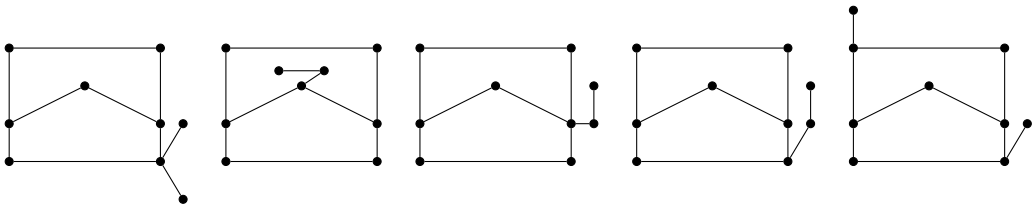
84



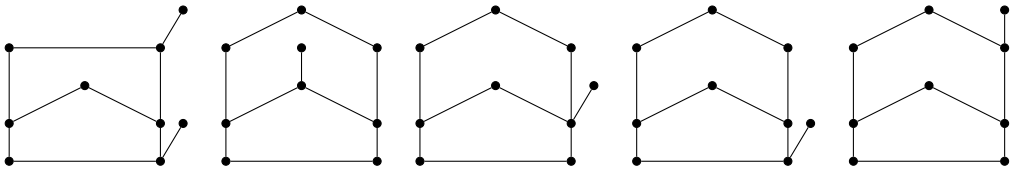
85 86 87 88



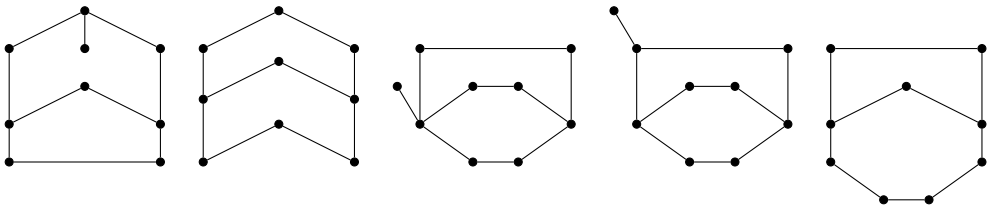
89 90 91 92 93



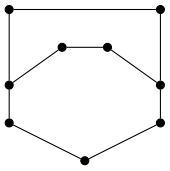
94 95 96 97 98



99 100 101 102 103

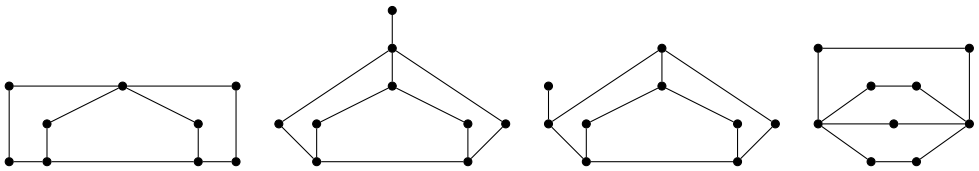


104 105 106 107 108

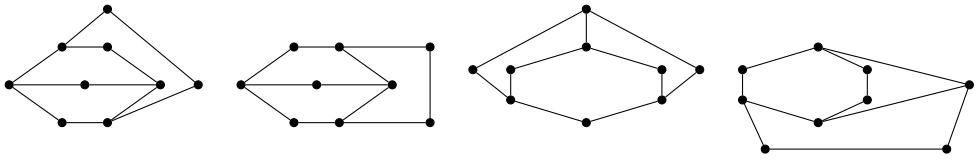


109

Gráfok 9 csúccsal és 11 éllel:



110 111 112 113



114 115 116 117

A fenti gráfok bonyolultságát az alábbi táblázat mutatja:

Bonyolultság	Sorszám
3/2	6, 23, 81
5/3	1, 2, 4, 5, 7, 8, 10, 11, 13, 15, 18, 20, 21, 22, 28, 30, 31, 36, 37, 40, 42, 44, 48, 50, 52, 62, 64, 65, 67, 70, 71, 73, 74, 76, 78, 79, 80, 104, 105, 108, 109
7/4	3, 9, 12, 14, 17, 19, 24, 25, 26, 29, 32, 33, 34, 35, 39, 41, 43, ,46, 47, 49, 51, 55, 56, 59, 60, 61, 63, 68, 69, 72, 77, 82, 85, 89, 90, 93, 94, 96, 97, 98, 101, 102, 103, 106, 107, 110, 113, 114, 116
9/5	16, 27, 45, 53, 55, 57, 58, 66, 83, 84, 86, 91, 95, 99, 100, 111, 115
11/6	38, 87, 88, 92, 117
13/7	112

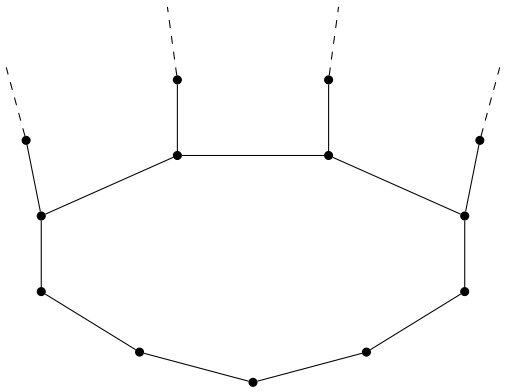
7.3.1. táblázat

8. fejezet

Új gráfcsalád meghatározott bonyolultsággal

A fákról és egy $2-1/d$ bonyolultságú gráfcsaládról az 5. valamint a 6. fejezetben írtam. A következőkben egy olyan gráfcsaládot mutatok be, amely sokban hasonlít ehhez a két gráfcsaládhoz.

Tétel 8.0.1 *Tegyük fel, hogy G olyan gráf, ami egy $h \geq 5$ hosszú körből és ennek a $k \leq h-5$ darab szomszédos csúcsából kiinduló diszjunkt útból áll (tehát az utak sem közös élen, sem közös csúcson nem osztoznak és egy-egy 1 fokszámú csúcsban érnek véget). Ekkor G bonyolultsága egyenlő* $2-1/(k+2)$.



8.0.1 ábra: Példa az új gráfcsaládra

Látható, hogy minden ilyen tulajdonsággal rendelkező G gráf esetén a csúcsok és az élek száma megegyezik, a maximum fokszám 3, és a 3 fokszámú csúcsok összefüggőek. Viszont a 6. fejezetben leírt gráfcsalád (B) tulajdonságát el tudtuk hagyni, a (C) tulajdonságot pedig gyengíteni. Továbbá vegyük észre, hogy ha a G-ben lévő körből egy tetszőleges élt elhagyunk, akkor fát kapunk valamint, hogy a fákhoz hasonlóan a bonyolultság ezeknek a gráfoknak az esetében is a legnagyobb mag elemszámának függvénye.

Bizonyítás. Legyen f a dolgozatban már többször alkalmazott, 4.1. fejezetben definiált függvény, amire teljesülnek az ott megfogalmazott a)-e) tulajdonságok. Ugyanebben a fejezetben igazoltuk, hogy egy gráf G minden X összefüggő csúcshalmazára teljesül a következő egyenlőtlenség:

$$\sum_{\{v\}\in X} f(v) \geq f(X) + |X| - 2. \tag{8.1}$$

Illetve korábban kimondtuk és bebizonyítottuk a "független szekvencia lemma"-t [7], [10]:

Lemma 8.0.2 *Tegyük fel, hogy $A = \{v_1, \ldots, v_n\}$ összefüggő és létezik $B = \{w_1, \ldots, w_n\}$ független halmaz úgy, hogy minden w_i pontosan egy v_i-vel van összekötve. Ekkor $f(A) \geq |A| + 1$.*

Ha egy gráfban találunk olyan A részhalmazt a csúcsok között, amire teljesülnek a lemma feltételei, akkor a lemmának és a 8.1-es egyenlőtlenségnek az összegéből következik, hogy van legalább egy olyan $v \in A$ csúcs, amire $f(v) \geq 2 - 1/|A|$. Ezt részletesebben levezettük az 5. fejezetben.

A tételben megfogalmazott feltevések miatt egyszerű ilyen A-t választani. Álljon A a $v_1, \ldots, v_k$ összefüggő 3 fokszámú csúcsból, valamint vegyük még hozzá a v_1 és v_k pontok h hosszú körön elhelyezkedő szomszédait. Az így megválasztott A részhalmaz mérete $k+2$ és teljesíti a lemma feltételeit, tehát igazoltuk, hogy $2 - 1/(k+2) \leq C(G)$.

Megjegyzés: A $k \leq h-5$ feltétel a tételben arra szolgál, hogy a független szekvencia lemmát használni tudjuk és így tudjunk megfelelő alsó korlátot találni, azonban az eredmények 7. fejezetben azt sugallják, hogy a tétel minden $k \leq h-1$ esetben igaz.

A felső korlát megtalálásához az 5. és 6. fejezet metódusát követjük, azaz a [6] eredményeinek segítségével bizonyítunk. Olyan csillagfedést fogunk építeni, ami minden élt $k+2$-ször és minden csúcsot $2(k+2)-1$-szer fed le. Minden G-beli élt helyettesítsünk $k+2$ darab irányított éllel, melyeknek irányát később szabjuk meg. A csillagfedést a már irányított élek alapján határozzuk meg úgy, hogy az élek minden esetben a csillag középpontjából kifelé indulnak. Ez azt jelenti, hogy minden $v \in G(V)$-ből kimenő él egy v középpontú csillag része, így annyi ilyen v csillagot készítünk, amennyi a v-ből egy szomszédjába maximálisan kimenő élek száma. Továbbá v annyi csillagnak a csúcsa, amennyi a v-be bejövő élek száma. A két szám összege $k+2$ plusz az összes bejövő élek száma, kivéve a bejövő élek száma abból a szomszédból, ahonnan a legkevesebb bejövő él érkezik.

Az éleket abból a szempontból fogjuk vizsgálni, hogy milyen fokszámú csúcsokat kötnek össze. Előtte azonban két esetet kell elkülönítenünk k paritása szerint.

I. eset: k páros, $k+2 = 2n$, azaz minden eredeti él helyén $2n$ darab élt kell irányítanunk.

(i) Azoknak az éleknek az esetében melyeknek egyik csúcsa 1 fokszámú, irányítsunk minden élt az 1 fokszámú a csúcs felé.

(ii) Az olyan élek esetén amelyek 2 db 2 fokszámú csúcsot kötnek össze, irányítsunk n darabot az egyik és n darabot a másik irányba.

(iii) Ha egy él egy 2 és egy 3 fokszámú csúcs között húzódik, akkor a helyére húzott $2n$ él közül irányítsunk $2n-1$-et a 2 fokszámú és 1-et a 3 fokszámú csúcs felé.

(iv) A 3 fokszámú csúcsokat összekötő élek utat alkotnak a gráfban. Számozzuk meg ezeket "számegyenes szerűen", tehát a középső ilyen él (páratlan számú ilyen él van) kapjon 0 sorszámot, A szomszédainak sorszáma legyen 1, ezek megmaradt szomszédainak 2, és így tovább, amíg az összes ilyen típusú élt be nem számoztuk. Irányítsuk az éleket úgy, hogy ha x az él sorszáma, akkor $n+x$ él tartson abba az irányba, ahol nála a nagyobb sorszámú éllel van közös csúcsa, a maradék $n-x$ pedig az ellenkező irányba. A mivel az út legkülső éleinek sorszáma $n-2$, ezeken az éleken $2n-2$ él mutat az út végpontjába és 2 él mutat az ellenkező irányba. A 3 fokszámú csúcsokat összekötő élek irányítását páros esetben a 8.0.1-es táblázat szemlélteti.

Sorszám	$n-2$	$n-3$	...	2	1	0	1	2	...	$n-3$	$n-2$
Élek iránya	$\xrightarrow[2]{}$ $\xleftarrow[2n-2]{}$	$\xrightarrow[3]{}$ $\xleftarrow[2n-3]{}$		$\xrightarrow[n-2]{}$ $\xleftarrow[n+2]{}$	$\xrightarrow[n-1]{}$ $\xleftarrow[n+1]{}$	$\xrightarrow[n]{}$ $\xleftarrow[n]{}$	$\xleftarrow[n-1]{}$ $\xrightarrow[n+1]{}$	$\xleftarrow[n-2]{}$ $\xrightarrow[n+2]{}$		$\xleftarrow[3]{}$ $\xrightarrow[2n-3]{}$	$\xleftarrow[2]{}$ $\xrightarrow[2n-2]{}$

8.0.1 táblázat

Minden élt és minden 1 fokszámú csúcsot $2n = k+2$ csillaggal fedtünk le. Minden 2 fokszámú csúcsot, aminek nincs 3 fokszámú szomszédja $3n = (3/2)k+3$ csillaggal. Továbbá minden 3 fokszámú csúcsot és minden 2 fokszámú csúcsot, aminek van 3 fokszámú szomszédja $4n-1 = 2(k+2)-1$ csillaggal. Ezzel sikerült az alsó korláttal azonos felső korlátot találnunk, páros k esetén.

II. eset: k páratlan és $k+2 = 2n+1$.

(i) Azoknak az éleknek az esetében, melyeknek egyik csúcsa 1 fokszámú, irányítsunk minden élt az 1 fokszámú a csúcs felé.

(ii) Az olyan élek esetén, amelyek 2 db 2 fokszámú csúcsot kötnek össze, irányítsunk $n+1$ darabot az egyik és n darabot a másik irányba úgy, hogy minden olyan csúcsba, amelynek csak 2 fokszámú szomszédai vannak, egyik oldalról n a másik oldalról pedig $n+1$ csúcs érkezzen.

(iii) Ha egy él egy 2 és egy 3 fokszámú csúcs között húzódik, akkor a helyére húzott $2n+1$ él közül irányítsunk $2n$-et a 2 fokszámú és 1-et a 3 fokszámú csúcs felé.

(iv) A három fokszámú csúcsokat összekötő élek ebben az esetben is utat alkotnak. Ismét "számegyenes szerűen" számozzuk őket. Mivel $k+2$ páratlan, most a 0-t kihagyjuk a számozásból. Az út közepén lévő 1-1 él az 1-es sorszámot kapja, szomszédaik a

2-es sorszámot, és így tovább, amíg az összes ilyen élt be nem számoztuk. Az éleket irányítsuk úgy, hogy $n+x$ mutasson a sorszámozásnak megfelelően növekvő irányba, a maradék $n-x+1$ él pedig az ellenkező irányba. Az út két legszélső éle esetében tehát $2n-1$ él fog az út külső csúcsába mutatni, 2 pedig befelé. A 3 fokszámú csúcsokat összekötő élek irányítását páratlan esetben a 8.0.2-es táblázat szemlélteti.

Sorszám	$n-1$	$n-2$	...	2	1	1	2	...	$n-1$	$n-2$
Élek	$\underset{2}{\longrightarrow}$	$\underset{3}{\longrightarrow}$		$\underset{n-1}{\longrightarrow}$	$\underset{n}{\longrightarrow}$	$\underset{n}{\longleftarrow}$	$\underset{n-1}{\longleftarrow}$		$\underset{3}{\longleftarrow}$	$\underset{2}{\longleftarrow}$
iránya	$\underset{2n-1}{\longleftarrow}$	$\underset{2n-2}{\longleftarrow}$		$\underset{n+2}{\longleftarrow}$	$\underset{n+1}{\longleftarrow}$	$\underset{n+1}{\longrightarrow}$	$\underset{n+2}{\longrightarrow}$		$\underset{2n-2}{\longrightarrow}$	$\underset{2n-1}{\longrightarrow}$

8.0.2 táblázat

Az összes élt és az 1 fokszámú csúcsokat $2n+1 = k+2$-ször fedtük le. Azokat a 2 fokszámú csúcsokat, amelyeknek mindkét szomszédja is 2 fokszámú $3n+2 = (3/2)(k+1)+2$ csillag fedi. A 3 fokszámú csúcsokat és azokat a két fokszámú csúcsokat, amelyeknek egyik szomszédja 3 fokszámú, pontosan $4n+1 = 2(k+2)-1$-szer fedtük le. Ezzel a bizonyítás teljes. □

Megjegyzés: Tegyük fel, hogy a körből induló egyik legszélső út hossza legalább 2. Ilyen esetben a $k \leq h-5$ feltételt $k \leq h-4$-re változtathatjuk. Ha pedig ez a feltevés mindkét szélső útra igaz, akkor a $k \leq h-3$ feltétel is elég. Ezt nem nehéz belátni, hiszen ilyen esetekben az alsó korlát kereséséhez használt A halmazba a körön lévő 2 fokszámú csúcs/csúcsok helyett a szélső utak legelső csúcsát vehetjük bele. A csillagfedés pedig, ugyanúgy működik, mint ahogy a tétel bizonyításában szerepel.

Irodalomjegyzék

[1] L. Csirmaz: Titokmegosztás gráfokon, Nyíregyházi kriptográfiai és diofantikus nap, http://www.renyi.hu/ csirmaz/ (2005).

[2] A. Shamir: How to share a secret, Communications of the ACM 22 (11): 612-613 (1979).

[3] G.R. Blakley: Safeguarding cryptographic keys, Proceedings of the National Computer Conference 48: 313-317 (1979).

[4] L. Csirmaz, P. Ligeti: On an infinite family of graphs with information ratio $2 - 1/k$, Computing, 85(1-2). pp. 127-136. ISSN 0010-485X (2009).

[5] P. Erdős, L. Pyber: Covering a graph by complete bipertite graphs, Discrete Mathematics, Vol 170 pp. 249-251 (1997).

[6] D.R. Stinson: Decomposition constructions for secret sharing schemes, IEEE Trans. Inform. Theory Vol 40 pp. 118-125 (1994).

[7] L. Csirmaz: Secret sharing schemes on graphs, Studia Mathematica, vol 44, pp. 297-306 (2007).

[8] L. Csirmaz: Secret sharing on the d-dimensional cube, https://eprint.iacr.org/2005/177

[9] L. Csirmaz, G. Tardos: Optimal information rate of secret sharing schemes on trees, Information Theory, IEEE Transactions on. ISSN 0018-9448 (2012).

[10] C. Blundo, G. Gaggia, D. R. Stinson: On the Dealer's Randomness Required in Secret Sharing Schemes, Designs, Codes and Cryptography, Vol 11(3), pp. 235-260 (1997).

[11] C. Bludo, A. Santis, R. Simone, U. Vaccaro: Tight Bounds on the Information Rate of Secret Sharing Schemes, Designs, Codes and Cyrptography, 11, 107-122 (1997).

[12] M. van Dijk: On the Information Rate of Perfect Secret Sharing Schemes, Des. Codes Cryptogr 6 pp. 143-160 (1995).

[13] C. Padro: Lecture Notes in Secret Sharing, IACR preprint http://eprint.iacr.org/2012/674

[14] W. Wang, Z. Li, Y. Song: The optimal information rate of perfect secret sharing schemes, Business Management and Electronic Information (BMEI), International Conference on, Vol 2 pp. 207-212 (2011).

[15] Y. Song, Z. Li, Y. Li, R. Xin: The optimal information rate for graph access structures of nine participants, Front. Comput. Sci. DOI 10.1007/s11704-015-3255-6 (2015).

[16] W. Jackson, K. M. Martin: Perfect secret sharing schemes on five participants, Designs, Codes and Cryptography, Vol 9, pp. 267-285 (1996).

[17] C. Padro, L. Vázquez, A. Yang: Finding lower bounds on the complexity of secret sharing schemes by linear programming, Discrete Applied Mathematics 161, pp. 1072-1084 (2013).

[18] Y. Song, Z. Li, W. Wang: The Information Rate of Secret Sharing Schemes on Seven Participants by Connected Graphs, Advanced Materials Research Volume 127, pp. 637-645 (2012).

[19] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro: On the size of shares of secret sharing schemes, Journal of Cryptology, vol 6, pp. 157-168 (1993).

Nyilatkozat

Név: Harsányi Károly
ELTE Természettudományi Kar, szak: Matematika BSc
Neptun azonosító: F0GI4A
Szakdolgozat címe: Titokmegosztás és a bonyolultság vizsgálata gráfokon

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

Budapest, 2015.05.29.

a hallagtó aláírása

Nyilatkozat

Név: Harsányi Károly
ELTE Természettudományi Kar, szak: Matematika BSc
Neptun azonosító: F0GI4A
Szakdolgozat címe: Titokmegosztás és a bonyolultság vizsgálata gráfokon

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

Budapest, 2015. 05. 29.

a hallagtó aláírása