Titokmegosztás gráfokon

Csirmaz László*

Nyíregyházi kriptográfiai és diofantikus nap
2005, április 30

Absztrakt

A G gráfon alapuló *tökéletes titokmegosztás* olyan rendszer, melynek segítségével a gráf csúcsai, vagyis a *résztvevők* között titokrészeket osztunk szét oly módon, hogy ha a résztvevők egy halmaza tartalmaz élt, akkor együttesen vissza tudják nyerni a titkot, míg ha nem tartalmaz élt, akkor az általuk birtokolt információ és az elrejtett titok statisztikailag független. A rendszer átlagos információs hányadosa a titok méretének és a résztvevők által megjegyzendő átlagos információ méretének hányadosa. A G gráf információs hányadosa a rajta alapuló titokmegosztási rendszerek hányadosainak szuprémuma. A cikkben azokat a módszereket mutatjuk be, melyekkel a d dimenziós kocka élhálózatának információs hányadosát kívánjuk meghatározni.

1 Bevezetés

Titokmegosztási rendszer egy olyan eljárás, melynek segítségével résztvevők egy (véges) halmazának elemei között résztitkokat osztunk szét oly módon, hogy a *kvalifikált* részhalmazok az általuk együttesen birtokolt részinformációk alapján a titkot vissza tudják állítani. Ha ezen kívül a nem kvalifikált részhalmazok semmilyen részinformációval nem rendelkeznek – vagyis az együttes résztitkaik statisztikailag független az elrejtett titoktól –, akkor *tökéletes* titokmegosztási rendszerről beszélünk. A rendszer jóságát azzal lehet mérni, hogy egy résztvevőnek átlagosan (vagy a legrosszabb esetben) mennyi információt kell megjegyeznie. Optimális rendszerek keresése mint elméleti mint gyakorlati szempontból fontos feladat. Gyakorlati szempontból minél kevesebb információt kell a résztvevőknek megjegyezni, annál biztonságosabb az eljárás. A legtöbb titokmegosztási rendszernél az ismert alsó és felső korlátok nagyon messze vannak egymástól. Bizonyos speciális esetekben is igen nehéz feladat a korlátokat egymáshoz közelíteni; általános esetben a két korlát hányadosa exponenciális, lásd például [5]. A [9] vagy [3] cikkekben a feladat hátteréről, gyakorlati és elméleti felhasználásáról lehet bővebb információt találni.

A dolgozat felépítése a következő. Elsőként pontos definíciót adunk a titokmegosztási rendszerekre. Különböző példákon illusztráljuk a definiált fogal-

*Közép-Európai Egyetem

makat. Majd ismertetjük az úgynevezett entrópia módszert, és bemutatjuk a módszer egy viszonylag egyszerű alkalmazását. Az utolsó részben a d dimenziós kocka élgráfjára vizsgáljuk; felső korlátot adunk a megjegyzendő bitek számára, és megmutatjuk hogy ez a korlát éles $d = 2$, $d = 3$ és $d = 4$ esetben. Vázoljuk a felmerülő lineáris programozási feladatot, mellyel a $d = 5$ eset kezelhető.

2 Definíciók

Ebben a részben pontosan definiáljuk a tökéletes titokmegosztási rendszereket, és mindjárt néhány példával illusztráljuk a legfontosabb fogalmakat.

Legyen P a résztvevők véges halmaza: $P = \{v_1, v_2, \ldots, v_n\}$. A *titokmegosztás* $n + 1$ darab (közös eloszlással rendelkező) valószínűségi változó. Az első ξ-vel jelölt értéke a *titok*, a többi n darab, ξ_1, …, ξ_n a *titokrész*, a ξ_i értékét egyedül a v_i résztvevő ismeri.

Ha a résztvevők egy $A \subseteq P$ halmaza *kvalifikált*, akkor az általuk birtokolt értékekből együttesen meg kell tudniuk határozni a titok értékét. Más szavakkal $\{\xi_i : i \in A\}$ meghatározza ξ-t. Ha viszont $A \subseteq P$ *nem kvalifikált*, akkor az A-beliek által ismert értékek és a titok statisztikailag függetlenek kell legyenek: $\{\xi_i : i \in A\}$ és ξ függetlenek. A kvalifikált részhalmazok összességét *elérési struktúrának* szokás nevezni, és $\mathcal{A}$-val jelölni.

Az 1. táblázat kilenc oszlopában a három titokrész és a titok lehetséges együttes értékeit tüntettük fel. Minden oszlop ugyanakkora valószínűségű, mégpedig 1/9. 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. Így a résztvevők egy elemű részhalmazai nem-kvalifikáltak.

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

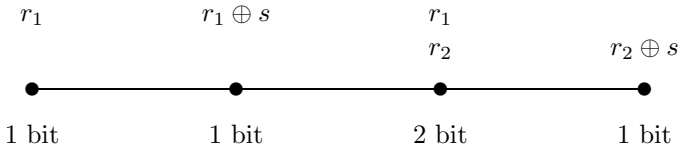
1. táblázat: titokmegosztás három résztvevővel

Ugyanakkor bármely két résztvevő együttes értéke már egyértelműen meghatározza a ξ titok értékét, következésképp bármely kételemű részhalmaz kvalifikált – és ekkor persze az ennél nagyobb részhalmazok is kvalifikáltak lesznek.

Mivel a minimális kvalifikált részhalmazok itt kételeműek, az elérési struktúrát egyértelműen jellemezhetjük azzal a gráffal, melyben két résztvevőt pontosan akkor köt össze él, ha ők együtt egy kvalifikált halmazt alkotnak. Ez a gráf éppen a háromszög.

Második példánkban az elérési struktúrát a három hosszúságú vonalgráf adja meg. Vagyis összesen négy résztvevő van, bármely két szomszédos kvalifikált részhalmazt alkot. A csúcsok bármely más, élet nem tartalmazó része pedig nem kvalifikált. Az 1. ábrán azt mutatjuk meg, hogyan lehet az s bitet szétosztani a résztvevők között. Az s titok valamint az r_1 és r_2 mindannyian véletlen bitek,

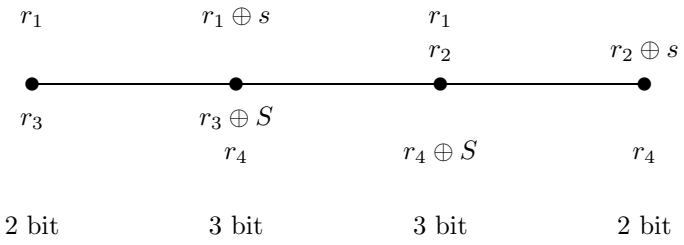
vagyis mindegyikük a többitől függetlenül 1/2 valószínűséggel veszi fel a 0 és 1 értékeket. $r_1 \oplus s$ a két bit modulo kettő összege, vagyis pontosan akkor 1, ha r_1 és s különböznek.



1. ábra: titokszétosztás vonalgráfon

A szétosztás megfelelő. Egyrészt a szomszédos résztvevők meg tudják kapni a titkot, az általuk birtokolt megfelelő bitek modulo kettő összege kiadja. A harmadik résztvevő két bitje közül a felsőt használja ha a bal oldali szomszédjával, és az alsót a jobb oldali szomszédjával. Ha pedig egy nem kvalifikált részhalmaz jön össze – például az első és az utolsó, akkor az általuk birtokolt bitek értékei függetlenek az s értékétől. Az is látható, hogy például az első és harmadik résztvevő értéke nem független (a harmadik résztvevő pontosan tudja mit kapott az első), de például az első és utolsó résztvevő által birtokolt értékek már függetlenek.

A szétosztást szimmetrikussá tudjuk tenni, ha a titok nem egy bit, hanem kettő, mondjuk s és S. A felosztást a 2. ábra mutatja. A két középső résztvevő

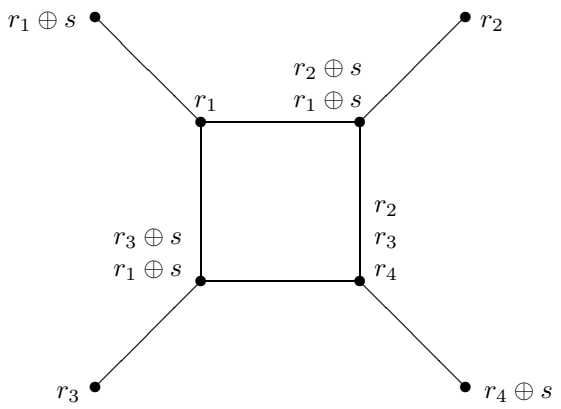


2. ábra: két bit elosztása szimmetrizálással

most három–három bitet jegyez meg, míg a két szélső kettőt–kettőt. Ennél a szimmetrizált titokmegosztásnál minden résztvevőnek titokbitenként legfeljebb másfél bitet kell megjegyezniük, míg az előző eljárásnál az egyik résztvevő a titok kétszeresét kapta.

A 3. ábrán úgy osztottuk szét az s egybites titkot, hogy a négy középső csúcshoz rendre 1, 2, 2 illetve 3 bitnyi megjegyzendő információ jut. Hasonlóan az előző szimmetrizálással kaphatunk olyan titokmegosztást, ahol mind a négyen a titok minden bitjére pontosan 2 bitnyi információt jegyeznek meg.

Célunk olyan titokmegosztás készítése, melyben ez a faktor – vagyis a legtöbb információt kapó résztvevő adatának mérete és a titok méretének hányadosa –



3. ábra: a középsők átlagosan két bitet jegyeznek meg

minél kisebb. Az összes megfelelő titokmegosztásra kiszámítjuk ezt a hányadost, és az így adódó értékek infimumát nevezzük a G gráf *információs hányadosának*, és $\mathrm{IH}(G)$-vel jelöljük. Megjegyezzük még, hogy az irodalomban az általunk bevezetett információs hányados reciprokát is szokás használni.

3 Felső korlát

Gráfok – és általában tetszőleges elérési struktúrák – információs hányadosának meghatározása mind elméleti mind gyakorlati szempontból fontos és gyakran reménytelen feladat. Általánosságban az sem ismert, hogy tetszőleges gráfra az infimumot valamilyen elérési struktúra felveszi-e. Minden egyes konstrukció egyúttal egy *felső korlát*ot is ad. Így például a fentiek alapján a háromszög információs hányadosa legfeljebb 1; a három hosszúságú úté legfeljebb $1,5$; a 3. ábrán látható gráfé pedig legfeljebb 2. Általánosabb konstrukciókat később fogunk ismertetni.

A teljes páros gráf információs hányadosa legfeljebb 1. A konstrukció a következő. Legyen V_1 és V_2 a teljes páros gráf két osztálya, vagyis ha V_1-ből és V_2-ből veszünk ki egy-egy csúcsot, akkor fut közöttük él, míg két V_1 (és két V_2-beli) között nem. A titok legyen az egyetlen s bit, r pedig egy véletlen bit. V_1 minden elemének mondjuk meg r-et, V_2 minden elemének pedig $r \oplus s$-et. Ezzel mindenki egyetlen bitet kapott, és a feltételek nyilván teljesülnek.

Jóval bonyolultabb az az eset, amikor G a teljes gráf, ám ilyenkor is adható konstrukció, ami mutatja hogy ebben az esetben is az információs hányados legfeljebb 1. A konstrukció leírásához vegyünk egy véges test fölötti véges dimenziós T vektorteret. Válasszunk egy $v \in T$ vektort, valamint minden $i \in P$ résztvevőhöz egy további v_i vektort. Tegyük fel, hogy ezek a vektorok rendelkeznek a következő tulajdonsággal. Ha $A \subseteq P$ egy kvalifikált rendszer, akkor

a $\{v_i : i \in A\}$ vektorok által kifeszített altérben benne van a v vektor; ha viszont $A \subseteq P$ nem kvalifikált, akkor v nincs ebben az altérben. Ezek után a titokszétosztás a következőképpen történik. Kivesszük a vektortér egy véletlen $r \in T$ elemét. Mivel T véges, ezt egyszerűen megtehetjük. Ezek után a titok a $v \cdot r$ skalárszorzat (az alaptest egy eleme), az $i \in P$ résztvevő titokrésze pedig a $v_i \cdot r$ skalárszorzat. Világos, hogy mindegyik titokrész ugyanakkora méretű mint a titok (és megegyezik az skalártér elemszámának kettes alapú logaritmusával). Ha most egy kvalifikált részhalmaz elemei jönnek össze, akkor a hozzájuk rendelt v_i vektorok valamilyen lineáris kombinációja kiadja v-t:

$$v = \sum \{\lambda_i v_i : i \in A\}$$

ahol a λ_i konstansokat a titokrészek ismerete nélkül is meg tudják határozni. Ezek után a skalárszorzat linearitása miatt

$$v \cdot r = \sum \{\lambda_i (v_i \cdot r) : i \in A\}$$

vagyis a titkot, azaz $v \cdot r$-et ki tudják számítani. Ha viszont A nem kvalifikált részhalmaz, akkor *azon feltétel mellett, hogy az összes $v_i \cdot r$ skalárszorzat értéke előre megadott*, a $v \cdot r$ skalárszorzat a skalártér minden elemét pontosan ugyanannyiszor veszi fel. Ez pedig éppen azt jelenti, hogy a titok értéke statisztikailag független a résztvevők titokrészétől.

Rátérve az n csúcsú teljes gráfra, válasszunk egy legalább $n+1$ elemű F véges testet, és az F feletti két dimenziós T vektortérben $n+1$ darab vektort úgy, hogy közülük bármely kettő kifeszítse a teljes vektorteret. Az egyik vektort választva v-nek, a többit a gráf csúcsaihoz rendelve éppen egy 1 információs hányadosú titokszétosztást kapunk, ahol a minimális kvalifikált halmazok éppen a résztvevők kételemű halmazai.

Ezeket használva tetszőleges gráfra tudunk felső korlátokat adni. Ha G lefedhető teljes páros gráfokkal úgy hogy minden csúcs legfeljebb k-ban van benne, akkor G információs hányadosa legfeljebb k. Annak alapján hogyan választjuk meg a teljes páros gráfokat, különböző korlátokat tudunk adni.

- Ha G-t az élekkel fedjük le, akkor adódik, hogy $\mathrm{IH}(G) \leq n-1$.
- Ha G-t a csúcsokból induló csillagokkal fedjük le, akkor $\mathrm{IH}(G) \leq d+1$, ahol d a gráf maximális foka.
- Ha G éleit megfelelően irányítjuk és az irányított csillagokat tekintjük, akkor $\mathrm{IH}(G) \leq (d+2)/2$ adódik.
- Stinson [9] egy ügyes konstrukcióval $\mathrm{IH}(G) \leq (d+1)/2$-t igazolt.
- Erdős és Pyber [8] megmutatta, hogy teljes párosokkal minden gráf lefedhető úgy, hogy minden csúcsot legfeljebb $c \cdot n/\log n$-szer fedünk le. Innen $\mathrm{IH}(G) \leq c \cdot n/\log n$, ami egy $\log n$-es faktorral javítja az első pontban kapott korlátot.

4 Alsó korlát

Hogyan tudjuk az információs hányadost *alulról* becsülni? A triviális esetek elkerülésére feltesszük, hogy G összefüggő. Ebben az esetben $\mathrm{IH}(G)$ legalább

1 kell hogy legyen. A bizonyítás a következő információelméleti észrevételen múlik. Ha ξ_2 és ξ függetlenek, akkor ahhoz, hogy ξ_1 és ξ_2 együttesen meghatározza ξ-t, az újonnan hozzávett ξ_1-ben legalább annyi (új) információnak kell lennie, mint amennyi ξ-ben van. Így ξ_1 mérete sem lehet kisebb a titok méreténél.

Ezt az informális okoskodást lehet precízzé tenni az *információelméleti módszerrel*. Ennek bemutatására emlékeztetünk arra, hogy egy η valószínűségi változó *entrópiája*

$$\mathbf{H}(\eta) \stackrel{\text{def}}{=} -p_1 \log_2 p_1 - \ldots - p_k \log_2 p_k,$$

ahol η a k különböző értékeket p_1, …, p_k valószínűséggel veszi fel. Esetünkben a résztvevők P halmazának *minden* A részhalmazára kiszámítjuk annak entrópiáját. Az így kapott $\{\mathbf{H}(A) : A \subseteq P\}$ összesség egy *polimatroid*, mert rendelkezik a következő tulajdonságokkal:

a) az üres halmazhoz rendelt érték nulla: $\mathbf{H}(\emptyset) = 0$, a többi érték nemnegatív: $\mathbf{H}(A) \geq 0$;
b) monoton: ha $A \subseteq B$, akkor $\mathbf{H}(A) \leq \mathbf{H}(B)$;
c) végül szubadditív: $\mathbf{H}(A \cup B) + \mathbf{H}(A \cap B) \leq \mathbf{H}(A) + \mathbf{H}(B)$.

Esetünkben a polimatroid még további speciális tulajdonságokkal is rendelkezik. Nevezetesen bizonyos esetekben az egyenlőtlenségek jobboldala jóval meghaladja a bal oldalt:

d) ha A nem kvalifikált részhalmaz, B igen, és $A \subseteq B$, akkor $\mathbf{H}(A) + \mathbf{H}(\xi) \leq \mathbf{H}(B)$;
e) ha A és B kvalifikált részhalmazok, míg $A \cap B$ 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 – ami egyúttal a titok mérete is. Az egyes résztvevők által megjegyzendő információ mérete éppen az egyelemű részhalmazok entrópiája. Így a rendszer információs hányadosa éppen a $\mathbf{H}(\xi_i)/\,\mathbf{H}(\xi)$ hányadosok maximuma.

Megjegyezzük, hogy a matroidok olyan speciális polimatroidok, melyek csak nem-negatív egész értékeket vesznek fel.

Ezzel a formalizmussal már be is tudjuk bizonyítani, hogy az információs hányados esetünkben mindig legalább egy. Legyen a és b a G gráf egy élének két csúcsa. Mivel a gráf összefüggő (és legalább két pontból áll), ilyeneket tudunk választani. Most az a és b egyelemű részhalmazok nem kvalifikáltak, míg az ab kételemű részhalmaz igen, tehát az e) tulajdonság miatt

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

A monotonitás miatt $\mathbf{H}(b) \leq \mathbf{H}(ab)$, ahonnan $\mathbf{H}(\xi) \leq \mathbf{H}(a)$. Ez pedig azt mondja, hogy a legalább annyi bitet kell megjegyezzen mint amennyi a titokban van *minden lehetséges titokmegosztási rendszerben*. Vagyis $\mathrm{IH}(G) \geq 1$, ahogyan állítottuk.

Az *információelméleti módszer* ezek alapján a következőképpen működik. Legyen adva egy G gráf. Megmutatjuk, hogy tetszőleges olyan polimatroidra,

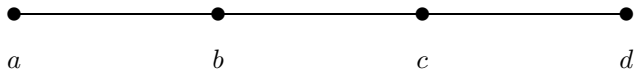
ami a d) és e) további tulajdonságokat is teljesíti, valamelyik egy elemű részhalmazhoz rendelt érték legalább $\kappa \cdot \mathbf{H}(\xi)$. Ekkor ezen résztvevő által megjegyzendő információ mennyisége legalább κ-szorosa a titok méretének. Következésképp minden G-n definiált titokmegosztási rendszerben lesz olyan résztvevő, akinek legalább κ-szoros információmennyiséget kell megjegyeznie, vagyis $\mathrm{IH}(G) \geq \kappa$.

Sajnos ez a módszer nem univerzális. Ennek fő oka, hogy nem minden polimatroid kapható meg valószínűségi változók entrópiájaként. Ezen az egy állításon kívül sajnos nagyon kevés ismert arról, hogyan is néznek ki az ilyen típusú polimatroidok. Például még az sem ismert, hogy az összes polimatroid között az így realizálhatóak zárt halmazt alkotnak-e vagy sem – ami miatt azt sem tudjuk például, hogy az $\mathrm{IH}(G)$ mindig elérhető-e. Ugyanakkor nem ismeretes semmilyen más módszer ami az $\mathrm{IH}(G)$-re alsó korlátot adna.

Mivel minden polimatroid egyenlőtlenség lineáris, ezért feltehetjük hogy $\mathbf{H}(\xi) = 1$, és így az egyelemű halmazokon adódó értékek közvetlenül az alsó korlátot adják meg.

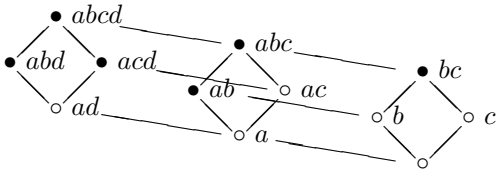
4.1. Tétel *A három hosszú út információs hányadosa* $1,5$.

Bizonyítás A fenti eljárás alkalmazzuk. Egészen pontosan azt mutatjuk meg, hogy a két középső résztvevőhöz rendelt értékek összege legalább három, vagyis



4. ábra: a résztvevők

$\mathbf{H}(b) + \mathbf{H}(c) \geq 3$. Azt, hogy melyik polimatroid egyenlőtlenségeket használjuk, az 5. ábrán mutatjuk be. Az ábrán üres körrel jelöltük azokat a részhalmazokat, melyek nem kvalifikáltak (mint például ac vagy ad), és tele körrel azokat, amik kvalifikáltak (például ab vagy $abcd$). A polimatroid d) tulajdonsága mi-



5. ábra: mit számoljunk?

att $\mathbf{H}(abcd) - \mathbf{H}(ad) \geq 1$. Az e) tulajdonságot az acd és abc halmazokra felírva, majd a szubadditivitást az ad és ac halmazokra (lásd az ábrát), a két egyenlőtlenség összege a következőképpen alakul:

$$\mathbf{H}(abc) - \mathbf{H}(a) \geq \mathbf{H}(abcd) - \mathbf{H}(ad) + 1.$$

Hasonlóan az e) tulajdonságot az ab és bc halmazokra, a szubadditivitást az a

és b halmazokra felírva kapjuk, hogy

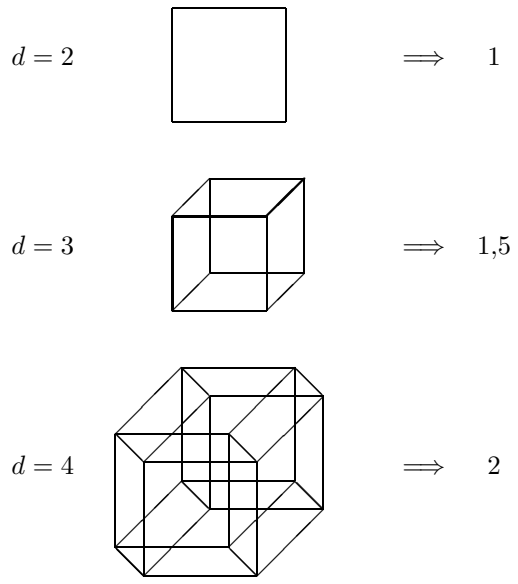
$$\mathbf{H}(bc) \geq \mathbf{H}(abc) - \mathbf{H}(a) + 1.$$

Végül megintcsak a szubadditivitás miatt $\mathbf{H}(b) + \mathbf{H}(c) \geq \mathbf{H}(bc)$. Ezt a négy egyenlőtlenséget összeadva éppen a kívánt egyenlőtlenséget kapjuk. ∎

5 A kocka

Ahogyan azt a 4. részben láttuk, Erdős és Pyber eredménye [8] szerint tetszőleges gráf információs hányadosa legfeljebb $c \cdot n/\log n$. Kérdés, hogy mekkora alsó korlátot tudunk biztosítani. A legjobb konstrukció [6]-ban található, ahol olyan n csúcsú gráfokat konstruáltunk, melynek információs hányadosa $c \cdot \log n$. Azt is sikerült bizonyítani, hogy a d dimenziós kocka élgráfjának információs hányadosa $(d+1)/2$ és $d/4$ közé esik. Mivel ennek a gráfnak az élszáma 2^d, azért ez a gráf is megadja a $c \cdot \log n$-es alsó korlátot.

Érdekes megoldatlan kérdésként merült fel, hogy határozzuk meg pontosan a d dimenziós kocka élgráfjának információs hányadosát. A $d = 2$ esetben a négyzet teljes páros gráf, így ennél a pontos érték 1, ahogyan az a 6. ábrán látható.



6. ábra: a 2, 3 és 4 dimenziós eset

A kockánál azt vehetjük észre, hogy feszített részgráfként a három hosszúságú út megtalálható benne. Ezért az információs hányadosa legalább akkora,

mint ennek a gráfnak, vagyis legalább $1,5$. Másik oldalról Stinson konstrukcióját ügyesen felhasználva tudunk $1,5$-ös titokmegosztási rendszert készíteni. Egy megfelelő F véges test feletti két dimenziós T vektortérben kiválasztunk hat vektort úgy, hogy közülük bármely kettő feszítse ki a teret. Ezeket a v_1, …, v_6 vektorokat hozzárendeljük a kocka *lapjaihoz*. A *titok* ennek a vektortérnek egy s véletlen eleme. Ha most az $s \cdot v_1$, …, $s \cdot v_6$ értékek közül kettőt ismerünk, akkor abból az s vektor már könnyen számítható. A kocka egy lapján négy csúcs van, mondjuk a laphoz tartozó vektor v_i. Az $s \cdot v_i$ skalárszorzatot szétosztjuk e négy résztvevő között: kettő átellenesnek az F test egy véletlen r elemét mondjuk, a másik kettőnek pedig az $r + (s \cdot v_i)$ mennyiséget. Mivel minden csúcs pontosan három lapon van, ezért minden résztvevő az F test három elemét jegyzi meg, a titok a test fölötti kétdimenziós vektortér egy eleme, tehát az információs hányados tényleg $1,5$. Az is világos, hogy egy él két végpontja együtt meg tudja határozni azokhoz a lapokhoz tartozó skalárszorzatokat, melynek mindkét csúcs rajta van, az összes többi skalárszorzatról viszont nincs semmilyen információjuk.

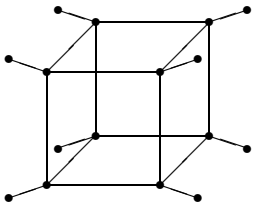
Ugyanez a konstrukció általában a d dimenziós kockára is elmondható; itt azt kell észrevennünk, hogy él a kockának $d-1$ darab kétdimenziós hipersíkján van, ezért az F test fölötti $d-1$-dimenziós vektortérből választunk vektorokat ezekhez a hipersíkokhoz. Minden csúcs $\binom{d}{2}$ 2-dimenziós hipersíkon van, tehát a testnek ennyi elemét kell megjegyezniük, míg a titok a test egy $(d-1)$-ese. A rendszer információs hányadosa tehát e két szám hányadosa, vagyis $d/2$. Az alábbi sejtést ezek szerint $d = 1$, 2 és 3 esetében igazoltuk, és azt is megmutattuk, hogy a kérdéses érték felső korlát is:

1. Sejtés *A d dimenziós kocka élvázának információs hányadosa éppen $d/2$.*

Hogyan lehet nagyobb dimenzióra ellenőrzni a sejtést? Alsó korlát megmutatására csak az információs módszer jöhet szóba. Ez viszont nem más, mint az a kérdés: a megfelelő polimatroid egyenlőtlenségekből milyen alsó korlát következik. A d dimenziós kockának 2^d csúcsa van, ezeknek 2^{2^d} részhalmaza. Így nagyságrendileg ennyi (maximum ennek negyedik hatványa) egyenlőtlenséget kell néznünk, melyek mindegyike egy egész együtthatós lineáris egyenlőtlenség. Ilyen feltételek mellett vagyunk kíváncsiak az összes egyelemű halmazhoz rendelt értékek összegének maximumára:

$$x_{\{1\}} + x_{\{2\}} + \ldots + x_{\{2^d\}} \to \mathrm{MAX}$$

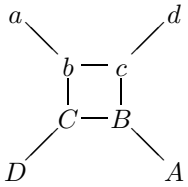
Így megfogalmazva a feladatot egy *lineáris programozási feladatot* kapunk. Mivel a csúcsok minden részhalmaza egy-egy változó, így például $d = 5$ esetben 2^{32} változónk van, és a redundáns egyenlőtlenségeket kiszűrve is legalább 2^{64} darab egyenlőtlenség. Ez a méret túl van azon, amihez érdemben hozzá lehet nyúlni. A $d = 3$ esetben az alsó korlát abból adódott, hogy a kocka élvázába feszített részgráfként a három hosszúságú út beágyazható. Az öt dimenziós kocka élvázába viszont a 7. ábrán látható gráf ágyazható be feszített részgráfként. Most azt kell csak megmutatnunk, hogy a középső kocka nyolc csúcsába kerülő értékek összege nagyobb mint $8 \cdot 2,5 = 20$. Ezzel a csúcsok számát 32-ről máris 16-ra redukáltuk, így a változók száma is lecsökkent 2^{16}-ra.



7. ábra: az 5 dimenziós kockába beágyazható gráf

A gráf szimmetriáit is figyelembe véve a változók száma tovább csökken 1995-re. Az egyenlőtlenségek száma – a redundánsakat kiszűrve – 46000 körüli. Ez utóbbi számot tovább tudjuk csökkenteni azzal, hogy ismerjük a feladat egy extremális megoldását, és csak azokat az egyenlőtlenségeket tartjuk meg, melyeknél az extremális megoldásban egyenlőség áll fenn. (Hogy ezt meg lehet tenni, a lineáris programozás elméletéből jól ismert; ez abból következik hogy a megoldásban egyetlen változó értéke sem lehet nulla.) Ezzel az egyenlőtlenségek száma 30475 lesz. Bár ez így redukált feladat még mindig nagyon nagy, de már nem reménytelen egy megfelelő lineáris programozási programmal való megoldása, hiszen az együttható mátrix nagyon ritka: egyenlőtlenségenként legfeljebb négy nem nulla együttható van.

A $d = 4$ esetben ez a lineáris programozási feladat néhány tucat változót és pár száz egyenlőtlenséget tartalmaz; ezt egy PC-n kevesebb mint három perc alatt lehet megoldani. Az egyes csúcsok jelölésére az $abcd$ és $ABCD$



8. ábra: a 4 dimenziós eset megoldása

betűket használjuk az ábrán látható módon. Mivel a gráf feszített részgráfként beágyazható a négydimenziós kockába (de a háromdimenziósba nem), elegendő megmutatnunk, hogy a négy középső résztvevő együttesen legalább nyolcszor annyi információt kell megjegyezzen, mint amennyi a titokban van. Ehhez pedig elég megmutatni, hogy $\mathbf{H}(bc) + \mathbf{H}(BC) \geq 8$, hiszen a szubmodularitás miatt $\mathbf{H}(b) + \mathbf{H}(c) \geq \mathbf{H}(bc)$, és hasonlóan $\mathbf{H}(B) + \mathbf{H}(C) \geq \mathbf{H}(BC)$. Az alábbi egyenlőtlenségek mindegyikét külön-külön könnyű ellenőrizni, összegük pedig éppen kiadja a kívánt alsó korlátot.

$$\begin{aligned} \mathbf{H}(AC) - \mathbf{H}(A) &\geq \mathbf{H}(abcAC) - \mathbf{H}(abcA) + 1 \\ \mathbf{H}(ac) - \mathbf{H}(a) &\geq \mathbf{H}(axABC) - \mathbf{H}(aABC) + 1 \end{aligned}$$

$$
\begin{array}{rcl}
\mathbf{H}(abcAC) - \mathbf{H}(aAc) & \geq & 2 \\
\mathbf{H}(axABC) - \mathbf{H}(acA) & \geq & 2 \\
\mathbf{H}(a) + \mathbf{H}(bc) & \geq & \mathbf{H}(abc) + 1 \\
\mathbf{H}(A) + \mathbf{H}(BC) & \geq & \mathbf{H}(ABC) + 1 \\
\mathbf{H}(abc) + \mathbf{H}(acA) & \geq & \mathbf{H}(ac) + \mathbf{H}(abcA) \\
\mathbf{H}(ABC) + \mathbf{H}(aAC) & \geq & \mathbf{H}(AC) + \mathbf{H}(aABC) \\
\hline
\mathbf{H}(bc) + \mathbf{H}(BC) & \geq & 8
\end{array}
$$

6 Összefoglalás

A tökéletes titokmegosztási rendszerek témakörének egyik fontos kérdése konkrét rendszerek információs hányadosának pontos meghatározása. Esetünkben a rendszert egy d dimenziós kocka csúcsai és (egydimenziós) élei jellemzik. A résztvevők a kocka csúcsai. A résztvevők egy részhalmaza akkor kell képesnek lenni visszaállítani a titkot, ha a részhalmaz tartalmaz élet; ha viszont a részhalmazban nincs él (vagyis a gráfelméletben szokásos kifejezéssel élve független), akkor az általuk együttesen birtokolt adatnak statisztikailag függetlennek kell lennie a titoktól. Ez az elrendezés azért érdekes, mert az információs hányadosa a résztvevők számának logaritmusa, ami az eddig bizonyított lehető legjobb alsó korlát gráfokra. Stinson [9] eredményét használva sikerült an információs hányadosra a $d/2$-es felső korlátot bizonyítani, és $d \leq 4$ esetére megmutatni hogy ez a pontos érték. Felvázoltuk azt, hogyan kiséreljük meg a $d = 5$ eset támadását. Azt reméljük, hogy az itt adódó rendszer a kisebb dimenziós esetekkel együtt már lehetővé teszi, hogy a sejtést, miszerint ez az érték mindig $d/2$, tetszőleges dimenzióra is bizonyítani tudjuk.

Irodalomjegyzék

[1] C. Blundo, A. De Santis, D. R. Stinson, U. Vaccaro: Graph Decomposition and Secret Sharing Schemes *Journal of Cryptology*, Vol 8(1995) pp. 39–64.

[2] E. F. Brickell and D. R. Stinson: Some improved bounds on the information rate of perfect secret sharing schemes *Journal of Cryptology*, Vol 5(1992) pp. 153–166.

[3] R. M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro: On the Size of Shares for Secret Sharing Schemes, *Journal of Cryptology*, Vol 6(1993) pp. 157-168.

[4] L. Csirmaz: The size of a share must be large, *Journal of Cryptology*, Vol 10(1997) pp. 223–231

[5] L. Csirmaz: The Dealer's Random Bits in Perfect Secret Sharing Schemes, *Studia Sci. Mathematica Hungarica*, Vol 32(1996) pp. 429–437

[6] L. Csirmaz: Secret sharing schemes on graphs, *Studia Sci. Mathematica Hungarica*, submitted

[7] M. van Dijk: On the Information Rate of Perfect Secret Sharing Schemes, preprint, 1994

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

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