Véletlen konstrukciók

Kisméretű teljes ívek véges projektív síkokon

Szakdolgozat

Írta: Vígh Dorottya

Alkalmazott Matematikus MSc
Sztochasztika szakirány

Témavezető:

Sziklai Péter, egyetemi docens
Számítógéptudományi Tanszék
Eötvös Loránd Tudományegyetem
Természettudományi Kar

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2012

Nyilatkozat

A szakdolgozat szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy az ELTE TTK Alkalmazott Matematikus MSc szak Sztochasztika szakirányán írt záródolgozatom önálló munkám eredménye, saját szellemi termékem, melyet korábban más szakon még nem nyújtottam be szakdolgozatként, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés, pontos hivatkozások nélkül nem használtam fel.

Fót, 2012. május 19.

Vígh Dorottya

Tartalomjegyzék

Bevezetés

1947-ben új eredmény született a Ramsey-számok elméletében: Erdős Pál alsó korlátot adott arra vonatkozóan, hogy legalább hány csúcsú teljes gráfra van szükségünk ahhoz, hogy a gráf éleit tetszőleges módon két színnel színezve (legyenek ezek piros és kék), legyen teljes r-es piros vagy teljes r-es kék színben (ezt a mennyiséget jelöljük $R(r,r)$-el). Tette mindezt úttörő módon[1] a valószínűségszámítás használatával. Ettől az időponttól kezdve egyre többen foglalkoztak az említett módszerrel, és sorra születtek az eredmények is – nagyszerű összefoglalását adja ennek a viszonylag új területnek Noga Alon és Joel H. Spencer könyve, a *The Probabilistic method* [1]. Szakdolgozatom célja is egy ilyen eredmény bemutatása lesz. Mielőtt azonban rátérnék a konkrét problémára, nézzük meg röviden, mi is az eljárás lényege.

A valószínűségi módszer egy nemkonstruktív metódus, ami egy bizonyos tulajdonságokkal rendelkező matematikai objektum létezését hivatott bizonyítani. A lényeg azonban nem az, hogy meg is konstruáljuk az említett objektumot: csupán azt látjuk be, hogy egy véletlen folyamat outputjaként pozitív (akár tetszőlegesen kicsi!) valószínűséggel megkapható. Tipikusan (Erdős nyomán) úgynevezett *egyfordulós* érvelést szokás használni, azaz generálunk egy alkalmas valószínűségi mezőt, majd megmutatjuk, hogy a kívánt objektumok halmaza pozitív mértékű ebben a térben. Igen gyakran ez a mérték 1 közeli, tehát bőven találhatunk a térben megfelelő elemeket.

A szakirodalomban *semi-random*, azaz *félvéletlen* módszernek nevezett eljárás Erdős eredeti gondolatmenetének egy kifinomultabb verziója: ennek segítségével ugyanis igen ritka objektumok létezését is igazolni tudjuk. Ebben az esetben a véletlenített algoritmust hosszabb időn át, több fordulóban futtatjuk, és belátjuk, hogy outputja pozitív valószínűséggel adja a keresett elemet. Ez a metódus az elmúlt évtizedekben számos áttörést eredményezett a kombinatorikában, komoly szerepet játszott általános gráfszínezési problémák megoldásában is (erről bővebben [12]-ben lehet olvasni). Szakdolgozatom alapját is egy erre az eljárásra épülő algoritmus adja.

[1] Habár korábban is születtek már tételek valószínűségi módszerek alkalmazásával – ilyen például Szele 1943-as eredménye Hamilton-köröket tartalmazó tournamentekről –, Erdős volt az, aki a legtöbb ismert bizonyítást adta ezen elv segítségével.

Egy másik lehetséges alkalmazása a valószínűségi módszernek, ha bizonyos valószínűségi változók várható értékét számoljuk ki. Ha például tudjuk, hogy a változó felvehet a várható értékénél kisebb értéket, ez bizonyítja, hogy annál nagyobbakat is elérhet. Más esetekben a változók átlagos viselkedése lehet fontos számunkra – ilyenkor a cél az, hogy belássuk: a valószínűségi változónk értékei erősen koncentrálódnak a várható értéke körül. Erre több módszer is ismert, az egyik legnevesebb és talán legtöbbet alkalmazott egyenlőtlenség Azuma nevéhez fűződik, amely korlátos differenciájú martingálok esetében ad koncentrációs eredményt.

Mint láthatjuk, a valószínűségi metódusnak széles körű alkalmazási lehetőségei vannak – ennek megfelelően a matematika számos területén találkozhatunk vele, így a számelmélet, a lineáris algebra, valós analízis, számítástudomány és legfőképpen a gráfelmélet, véges geometria eredményeiben. Szakdolgozatomban is egy véges geometriai problémára, a teljes ívek minimális számosságára keressük a választ – a valószínűségi módszer, speciálisan a félvéletlen metódus és a várható érték körüli koncentráció segítségével. Látni fogjuk, hogy a korábban említett Azuma-egyenlőtlenség és egyéb, más esetekben nagy sikerrel alkalmazott becslések alkalmatlanok lesznek a feladat megoldására, ezért egy viszonylag új koncentrációs eredményt is bemutatok a dolgozatomban, amely számos további lehetőséget is rejt magában, erről bővebben V. H. Vu *Concentration of non-Lipschitz functions and applications* [12] című cikkében lehet olvasni.

A dolgozat alapját képező probléma a következő: ha adott egy $\mathcal{P}$ projektív sík, határozzuk meg a lehető legkisebb teljes ív méretét benne, ahol ív alatt olyan ponthalmazt értünk, melyben semelyik három pont nincs egy egyenesen, a teljesség pedig szokásos módon azt jelenti, hogy a ponthalmaz nem bővíthető a feltétel megsértése nélkül. A keresett mennyiséget $n(\mathcal{P})$-vel jelöljük. A problémakört az 1950-es évek végén Beniamino Segre, olasz matematikus vetette fel ([9]), aki a teljes ívek maximális számosságát kutatta – azonban a másik irány, a lehető legkisebb méret érdekesebbnek bizonyult az eredeti kérdésfelvetésnél. Több mint 50 évvel ezelőtt Lunelli és Sce q-rendű $\mathcal{P}$ esetén $\sqrt{2q}$-s alsó határt állapított meg ([8]), azonban ettől az eredménytől eltekintve semmit nem lehetett tudni $n(\mathcal{P})$-ről a Galois-sík esetét leszámítva (erre Szőnyi Tamás adott $O(q^{3/4})$-es becslést ([10])). A dolgozatban bemutatásra kerülő fő tétel tetszőleges $\mathcal{P}$ q-rendű projektív síkra $\sqrt{q}\log^c q$-s felső korlátot ad, ahol c egy univerzális konstans. Lunelli és Sce alsó korlátjával együtt ez már egy polilogaritmikus faktor erejéig meghatározza $n(\mathcal{P})$-t. Ahogy korábban már említettem, a valószínűségi módszerek nemkonstruktívak, így a bizonyításhoz használt Rödl-féle „kiharapós" módszer (ezzel a következő fejezetben ismerkedünk meg) eredménye sem egy kézzelfogható konkrét ív lesz.

Szakdolgozatom alapját J. H. Kim és V. H. Vu *Small complete arcs in projective planes* [7] című cikke képezte, a dolgozatban megjelenő valamennyi tétel, állítás, lemma és következmény a szerzőpáros saját eredménye – a későbbiek során ezt az egyszerűség kedvéért

nem fogom külön feltüntetni. Fő feladatom az említett (közel 55 oldalas) publikáció értő, alapos feldolgozása, javítása volt. Ennek során az eredeti cikk több bizonyítását korrigáltam (így például a 4.6-os lemmáét, az első fázis **(6)**-os, majd az arra épülő, a második fázis **(3)**-as tulajdonságának alapvetően hibás bizonyítását stb.), több helyen kiegészítéseket, magyarázatokat, példákat illesztettem be a könnyebb érthetőség érdekében. A fentebb említett cikk mellett egyéb, valószínűségi módszerekkel, koncentrációs eredményekkel foglalkozó kiadványokkal is dolgoztam ([12], [6], [1]).

1. fejezet

A teljes ívek rövid története

Mielőtt belevágnánk szakdolgozatom központi eleme, a teljes ívek vizsgálatába, röviden átismételjük a legszükségesebb ismereteket a projektív síkokról. Egy q-rendű projektív sík q^2+q+1 pontot, valamint q^2+q+1 egyenest tartalmaz, ahol minden egyenesnek pontosan $q+1$ pontja van, és két különböző pontra pontosan egy egyenes illeszkedik. A definícióból könnyen levezethető, hogy minden ponton $q+1$ egyenes megy át, és két különböző egyenesnek pontosan egy közös pontja van. A legfontosabb példát projektív síkra talán a Galois-sík adja, melyet a következőképpen konstruálhatunk meg: legyen V a háromdimenziós vektortér a $GF(q)$ Galois-test felett, ahol q prímhatvány. A pontok és az egyenesek az egy- és kétdimenziós alterei V-nek, ahol egy p pont pontosan akkor illeszkedik egy l egyenesre, ha p altere l-nek. Ismert, hogy nagy q-kra sok q-rendű sík van, ami nem izomorf a Galois-síkkal, azonban nem tudni, hogy nem prímhatványrendű projektív síkok léteznek-e.

Ívnek a sík olyan ponthalmazát nevezzük, melyben semelyik három pont nincs egy egyenesen, teljes ív alatt pedig a nem bővíthető íveket értjük, ahogy ezt már a bevezetőben említettem. Azokat az egyeneseket, melyek az ív két pontját tartalmazzák, szelőnek nevezzük. Definíció szerint egy ív pontosan akkor teljes, ha szelői lefedik az egész síkot. Segre eredeti kérdése az volt, hogy egy teljes ívnek legfeljebb hány pontja lehet – könnyű látni, hogy $q+2$, Segre pedig bizonyította, hogy páratlan q-ra a Galois-sík íve legfeljebb $q+1$ pontból állhat, és a maximumot csak kúpszelettel lehet elérni, azaz olyan (x,y,z) pontokból álló halmazzal, melyekre teljesül, hogy $xz=y^2$. Páros q-ra a maximum $q+2$, de ezen ívek karakterizációja még mindig nem teljes. A figyelem tehát hamar átfordult a másik irányba: minimum hány pontja lehet egy teljes ívnek? A bevezetőben már említett alsó korlát könnyen igazolható: vegyük észre, hogy egy teljes ív szelői mind a q^2+q+1 pontot le kell fedjék, és mivel minden szelő $q+1$ pontot fed le, ezért egy teljes ívnek legalább $(q^2+q+1)/(q+1) \geq q$ szelője kell legyen. Ehhez viszont az ívnek legalább $\sqrt{2q}$ pontja kell legyen. Ezt az eredményt Blokhuis ([4]) és Ball ([3]) később $\sqrt{3q}$-ra javította a Galois-sík esetében, ha q prím vagy prímnégyzet. Fisher ([5]) sejtése szerint (melyet számí-

tógépes szimulációk támasztottak alá) a teljes ívek átlagos mérete körülbelül $(3q \log q)^{1/2}$, és mások Galois-síkokkal kapcsolatos munkái is azt a sejtést támasztották alá, hogy $n(\mathcal{P})$ pontos értéke $q^{1/2}$ környékén mozoghat. A szakdolgozatom alapját képező cikk megjelenéséig azonban nem sikerült ezeket a sejtéseket az általános esetben igazolni. Dolgozatomban viszont egy olyan eredményt fogok bemutatni, amely az általános síkokra vonatkozóan is jelentősen javítja $n(\mathcal{P})$ felső korlátját. A fő tétel a következő:

1.1. Tétel *Léteznek olyan pozitív c és M konstansok, hogy minden olyan q-rendű projektív síkban, melyre $q \geq M$, létezik legfeljebb $q^{1/2} \log^c q$ méretű teljes ív.*

Az 1.1-es tételt valójában nem közvetlenül bizonyítjuk, hanem egy erősebb eredmény igazolásával nyerjük:

1.2. Tétel *Léteznek olyan c és M abszolút konstansok, hogy minden olyan q-rendű projektív síkban, melyre $q \geq M$, található $\Theta(q^{1/2} \log^{1/2} q)$ pontú ív, melynek szelői $q^{1/2} \log^c q$ pont kivételével a sík összes pontját fedik.*

Az 1.2-es tétel bizonyítása során bemutatunk egy hatékony véletlenített algoritmust, ami a kívánt ívet 1 közeli valószínűséggel nyújtja számunkra. Az algoritmus alapvető műveletei közé tartozik leellenőrizni, hogy három pont egy egyenesre esik-e; pontot törölni egy egyenesről, illetve további hasonló lépések, ezekről az algoritmus leírásánál, a második fejezetben olvashatunk.

1.3. Tétel *Létezik egy olyan $\Theta(\log^{5/2} q)$ lépésigényű véletlenített algoritmus, ami $1-o(1)$ valószínűséggel előállítja az 1.2-es tételben szereplő ívet.*

Az 1.2-es tétel következményeként kapjuk az alábbit is:

1.4. Következmény *Léteznek olyan c_1, c_2, M pozitív konstansok, hogy minden olyan q-rendű projektív síkban, melyre $q \geq M$, van olyan teljes ív, melynek mérete $c_1 q^{1/2} \log^{1/2} q$ és $q^{1/2} \log^{c_2} q$ között van.*

Az 1.2-es tétel bizonyításához dinamikus véletlen konstrukciót, azaz félvéletlen metódust használunk (speciálisan Rödl „kiharapós" módszerét), melynek leírása a következő szakaszban található. A 3. fejezetben szerepel a fő lemmánk és az 1.2-es tétel bizonyítása a lemma segítségével. A 4. fejezetben a fő lemma igazolásához szükséges eszközöket vezetjük be, beleértve a korábban már említett koncentrációs eredményt. Végül az 5. fejezetben szerepel a fő lemma bizonyítása, amit az összefoglalás követ majd. Dolgozatom során mindvégig feltesszük, hogy q megfelelően nagy, ha szükséges. Az aszimptotikus jelöléseket, mint pl. Θ, O stb. a $q \to \infty$ feltételezés mellett értjük.

2. fejezet

Véletlen konstrukció

2.1. A „kiharapós” módszer

Mint az az előző fejezetből kiderül, az 1.2-es tételben szereplő ívet egy véletlenített algoritmus segítségével kaphatjuk meg. Az algoritmus alapját a „kiharapós” módszer képezi, amely igen erős és hatékony eszköze a valószínűségi kombinatorikának. A következőben ezt a metódust szeretném röviden bemutatni.

Szemben a véletlen mohó algritmussal, ami a véletlenszerűen sorbarendezett elemeket egymás után választja ki, feltéve, hogy nem sértik a feltételeket, amivel a kívánt objektumnak rendelkeznie kell; majd minden lépésben törli mindazon elemeket, amik a már kiválasztottakkal „ütközést” okoznának (esetünkben tehát egy üres halmazból kiindulva minden lépésben törölné a sík azon pontjait, amelyek a már kiválasztott pontok szelői által fedésben vannak, majd a maradék pontok közül egyenletes eloszlás szerint választaná a következő pontját az ívnek), egy lépésben egyszerre, egymástól függetlenül több pontot választunk ki (értelemszerűen a korábban még ki nem választottak közül). Ez a ponthalmazt nevezzük „harapás”-nak (a szakirodalomban *nibble* néven találkozhatunk vele). Tesszük ezt mindezt azért, mert bár sok esetben a sejtések szerint a mohó algoritmus majdnem optimális végeredményt ad, azonban ennek bizonyítása igen nehéznek bizonyul – mindmáig nem járt sikerrel. Az utóbb bevezett dinamikus véletlen konstrukció (DRC) hatékonyabbnak bizonyult a probléma megoldásában. A „kiharapott” ponthalmaz mérete vagy a kiválasztott pontok száma, vagy azok várható értéke. Mivel a kiválasztott ponthalmaz sértheti a feltételeinket, csak egy részhalmazát vesszük majd, ami eleget tesz azoknak. Ennek a részhalmaznak az elemeit nevezzük kiválogatottaknak. Az egyszerűség kedvéért azokat a kiválasztott elemeket, melyek a korábban és az aktuálisan kiválasztottakkal nem ütköznek (azaz együttesen nem sértik a feltételeket), általában kiválogatjuk. Törlünk minden olyan nem kiválasztott elemet, amely a választottakhoz adva ütközést okozna (tekintet nélkül arra, hogy a választottaknak végül mely részhalmazát válogatjuk ki). Mivel végül nem minden kiválasztott elemet fogunk kiválogatni, lesznek pontok, melyeket szükségtele-

nül törlünk, de a törlés-operációt úgy fogjuk bevezetni, hogy a rendelkezésre álló pontok struktúrája minden lépésben jóldefiniált legyen, és a független és véletlen kiválasztás elve érvényesülhessen. A következő lépésben további új feltételeket vezethetünk be. Így például a teljes ív esetén a kezdeti feltételünk az lehet, hogy semelyik három pont ne legyen egy egyenesen, míg az első „harapás" után hozzá kell adnunk azt a feltételt is, hogy semelyik két pont nem lehet már kiválasztott pontra illeszkedő egyenesen.

Az eljárás helyességének igazolásához meg kell mutatnunk, hogy a „harapás" méretének alkalmas megválasztásával pozitív valószínűséggel tudjuk az algoritmust mindaddig futtatni, amíg a kívánt objektumot el nem értük. Ha a „harapás" mérete túl nagy, azaz sok kiválasztott elem ütközik, két problémával is szembesülünk: nehéz lesz megjósolni a kiválasztott pontok struktúráját, továbbá túl sok pontot fogunk feleslegesen törölni. Éppen ezért a „harapás" méretének elég kicsinek kell lennie ahhoz, hogy a pontok többsége ne okozzon ütközést, így a feleslegesen törölt pontok száma is alacsony marad. Például ha egy q-rendű síkból $\theta q^{1/2}$ véletlen pontot választunk, annak valószínűsége, hogy tetszőleges kiválasztott pont ütközést okoz, legfeljebb $(q+1)\binom{q}{2}(\theta q^{-3/2})^2 \leq \theta^2$. (Ehhez ugyanis arra van szükség, hogy a pontra illeszkedő egyenesek valamelyikéről két másik pontot is kiválasszunk. Egy pontra $q+1$ egyenes illeszkedik, ezeken önmagán kívül további q pont van, végül pedig annak valószínűsége, hogy egy pontot beválasztunk, nagyságrendileg $\theta q^{1/2}/q^2 = \theta q^{-3/2}$.) Így amíg θ értéke kellően kicsi, a legtöbb pont nem fog konfliktust okozni. Természetesen abban az esetben, ha a „harapás" mérete minden lépésben egy, a DRC éppen a véletlen mohó algoritmust adja vissza.

A fentebb ismertetett terv véghezvitelének legkritikusabb része megmutatni, hogy minden lépés után a visszamaradó struktúra pozitív valószínűséggel az eredetinek véletlen részstruktúrájához hasonló. Ehhez általában elegendő néhány fontos paraméterről (esetünkben például egy egyenes túlélő pontjainak számáról) megmutatni, hogy éppen úgy viselkednek, ahogy azt a várható értékük jövendöli. Ennek igazolásához azonban olyan erős koncentrációs eredményre van szükségünk, amit a klasszikus eszközök az algoritmusunk komplexitása miatt képtelenek biztosítani. Ez a felismerés vezette az eredeti cikk szerzőpárosát egy új és saját eljárás kidolgozásához, amivel a 4. fejezetben fogunk majd megismerkedni.

2.1.1. Hogyan „haraphatunk" jó ívet?

Az algoritmusunk, melynek célja adott síkon egy kisméretű teljes ív konstruálása, nagyjából a következők szerint halad: kezdetben Ω_0 és S_0 jelöli a sík összes pontjából álló halmazt, A_0 pedig, melyet a kívánt ívvé fogunk kibővíteni, üres. Általánosan Ω_i azon pontok halmaza, amelyeket az aktuális A_i ív szelői nem fednek, S_i pedig Ω_i részhalmaza. Az i-edik lépésben, S_i minden pontját egymástól függetlenül ugyanazzal a p_i valószínűséggel választva létrehozzuk S_i-nek egy véletlen B_i részhalmazát. Majd B_i egy alkalmas részét A_i-hez adjuk úgy, hogy az új halmaz, A_{i+1} továbbra is ív maradjon. Ω_{i+1}-et mindazon pontok törlésével

kapjuk Ω_i-ből, melyeket A_{i+1} szelői fednek. S_{i+1} definiálásához nemcsak azokat a pontokat töröljük S_i-ből, melyeket A_{i+1} szelői fednek, hanem további véletlenszerűen választottakat is. Ennek az extra törlésnek az a célja, hogy S_i bizonyos strukturális jellegzetességeit minden lépésben megtartsuk.

Az eljárást addig ismételjük, míg $q^{1/2}\log^c q$ pont kivételével a sík összes pontját fedik az aktuális ív szelői (lásd az 1.2-es tételt). Az ötlet megvalósítása azonban rengeteg technikai részletet követel, ezekről a következő szakaszban lesz szó.

2.2. Az algoritmus

Az inputunk egy q-rendű $\mathcal{P}$ sík. Kezdetben Ω_0 és S_0 a sík összes pontjából állnak, A_0 pedig üres. Két futó paramétert is bevezetünk, a_i-t és b_i-t, ahol $a_0 = 0$ és $b_0 = 1$. Egy általános lépésben $a_i = |A_i|q^{-1/2}$ és b_i nagyjából $|S_i|/|S_0|$. Legyen $\theta = \log^{-2} q$.

Feltéve, hogy az i-edik lépés után Ω_i-t, S_i-t és A_i-t úgy konstruáltuk meg, hogy az A_i szelői által fedett pontok sem Ω_i-ben, sem S_i-ben nincsenek jelen, a következő műveleteket hajtjuk végre az $i+1$-edik lépésben:

Kiválasztás: Tetszőleges $v \in S_i$ pontot $p_i = \theta(b_i q^{3/2})^{-1}$ valószínűséggel választunk ki, jelölje B_i ezek halmazát. Egy $x \in B_i$ pontot *jó*nak nevezünk, ha nem okoz ütközést $A_i \cup B_i$-ben, azaz $A_i \cup B_i$ semelyik másik két pontja nem esik egy egyenesbe vele. Mivel S_i egyetlen pontját sem fedik A_i szelői, x pontosan akkor jó, ha

- nincsenek olyan $y \in B_i$ és $z \in A_i$ pontok, hogy x, y és z egy egyenesre illeszkedik,
- nincs olyan $y, z \in B_i$, hogy x, y és z egy egyenesen van.

Jelölje M_i a jó pontok halmazát, az új ív pedig legyen $A_{i+1} = A_i \cup M_i$.

Törlés: Töröljük Ω_i-ből mindazon pontokat, melyek vagy B_i-ben vannak, vagy A_{i+1} szelői által fedettek. Mivel Ω_i egyetlen pontját sem fedik A_i szelői, egy $v \in \Omega_i$ pontot pontosan akkor törlünk, ha

- $v \in B_i$,
- van olyan $x \in M_i$ és $y \in A_i$, hogy x, y és z egy egyenesen vannak,
- van olyan $x, y \in M_i$, hogy x, y és z egy egyenesre illeszkedik.

Jelölje D_i a fenti művelet során törölt pontok halmazát. Tetszőleges $v \in \Omega_i$ esetén jelölje $P_i(v) = P(v \in D_i)$, valamint legyen P_i^u és P_i^l a $P_i(v)$ értékek maximuma, illetve minimuma.

Kompenzáció: S_{i+1} definiálásához töröljük S_i-ből D_i minden pontját, továbbá ettől függetlenül tetszőleges $v \in S_i$ pontot

$$P_i^{com}(v) := (P_i^u - P_i(v))/(1 - P_i(v))$$

valószínűséggel. Jelölje R_i a törölt pontok halmazát. A következő lépéshez legyen

$$\Omega_{i+1} = \Omega_i \setminus D_i, \quad S_{i+1} = S_i \setminus (D_i \cup R_i), \quad A_{i+1} = A_i \cup M_i,$$

továbbá

$$a_{i+1} = |A_{i+1}|q^{-1/2}, \quad b_{i+1} = b_i(1 - P_i^u).$$

Az $i+1$-edik lépés után egy v pontot *túlélő*nek nevezünk, ha $v \in S_{i+1}$, és *nem törölt*nek, ha $v \in \Omega_{i+1}$. Értelemszerűen minden túlélő pont egyben nem törölt pont is. A fentiek alapján pedig nyilvánvaló, hogy annak valószínűsége, hogy egy $v \in S_i$ pont túlélő pont, éppen $1 - P_i^u$.

Megállás: Az algoritmus N lépés után megáll, ahol N az első olyan index, melyre $b_N \leq q^{-3/2}\log^c q$ valamely c konstansra (később c értékét 300-nak fogjuk választani).

Az algoritmus megállásakor egy A_N ívet kapunk. Az 1.2-es tétel igazolásához azt kell megmutatnunk, hogy ennek az ívnek $\Theta(q^{1/2}\log^{1/2} q)$ pontja van és szelői $O(q^{1/2}\log^c q)$ pont kivételével a sík összes pontját fedik. Az algoritmus jelöléseinek megfelelően az A_N szelői által nem fedett pontok $\Omega_N \bigcup(\cup_{i=1}^N B_i \setminus M_i)$ részhalmazát alkotják.

Célunk elérése érdekében az algoritmust két fázisban fogjuk vizsgálni aszerint, hogy $b_i \geq q^{-1}\log^{c_1} q$ vagy sem, ahol c_1 egy c-nél szignifikánsan kisebb konstans (értékét később 100-nak fogjuk választani). Minden fázisban több paramétert fogunk figyelni, úgy mint a nem törölt pontok száma egy egyenesen, az aktuális ív mérete stb., és belátjuk, hogy ezek a mennyiségek lényegében a várható értékük körül koncentrálódnak. Ez a lépés lesz a bizonyításunk fő feladata, és ehhez lesz szükségünk a korábban már említett új koncentrációs eredményre. Ha a paramétereket kezelni tudjuk, A_N kívánt tulajdonságai már egy egyszerű számításból következnek majd.

Megjegyzés: Láthatjuk, hogy a fentebb ismertetett algoritmus szorosan követi a DRC módszerét, csupán a kompenzáció lépése jelent eltérést. Tudjuk azonban, hogy egy pont törlésének valószínűsége az adott pont geometriai elhelyezkedésétől is függ, ezért a $P_i(v)$ törlési valószínűségek nem feltétlenül egyenlők minden v-re. Másrészt viszont az a célunk, hogy S_{i+1}-et S_i véletlenszerű részhalmazaként definiálhassuk, ezért arra van szükségünk, hogy minden S_i-beli pont ugyanakkora eséllyel maradhasson meg S_{i+1}-ben, avagy minden S_i-beli pontot azonos valószínűséggel töröljünk. A $P_i^{com}(v)$ kompenzációs valószínűséget pontosan ezért vezettük be.

2.3. Jelölések

Három különböző x, y, z pont esetén $[xyz]$-vel (néha, az indexek miatti zavart elkerülendő $[x, y, z]$-vel) jelöljük, hogy egy egyenesen helyezkednek el. Ezt a jelölést főleg összegzésekben használjuk majd, például $\sum_{j,j':[xjj']} t_j t_{j'}$ a $t_j t_{j'}$ szorzatok összege minden olyan j, j' párra, melyre j, j' és x egy egyenesen vannak. A két pontra, x és y-ra illeszkedő egyértelmű

egyenest (xy)-nal jelöljük. Tetszőleges $v \in \Omega_i$ pontra jelölje $A_i(v)$ a v-t A_i-beli pontokkal összekötő egyeneseken levő túlélő pontok halmazát (kivéve v-t magát). Formálisan

$$A_i(v) = \{x \in S_i \setminus v \mid \exists u \in A_i : [vxu]\}.$$

Kezdetben $A_0(v) = \emptyset$ minden v-re. Általánosan tetszőleges $X = \{v_1, \ldots, v_k\}$ ponthalmazra $A_i(X) = A_i(v_1, \ldots, v_k) := \cap_{j=1}^{k} A_i(v_j)$. Ugyanezt B_i-vel is definiáljuk: $B_i(v)$ a v-t B_i-beli pontokkal összekötő egyeneseken levő túlélő pontok halmaza. A $B_i(X)$ halmazt hasonlóan adhatjuk meg. Időnként a túlélő pontok helyett a nem törölt pontokra lesz szükségünk, jelölje tehát

$$A'_i(v) := \{x \in \Omega_i \setminus v \mid \exists u \in A_i : [vxu]\}.$$

Legyen továbbá $T_i(v)$ a v-vel egy egyenesen levő túlélő pontok (rendezetlen) párjainak halmaza. Formálisan

$$T_i(v) = \{\{x, y\} \mid x, y \in S_i \setminus v, [vxy]\}.$$

Kezdetben $T_0(v)$ minden v-re $(q+1)\binom{q}{2}$ párból áll.

Egy l egyenesre jelölje $S_i(l)$ l túlélő pontjainak halmazát, azaz $S_i(l) = S_i \cap l$. Ha az $S_i(l)$ jelölést használjuk, mindig feltesszük, hogy l nem szelő, hiszen különben $S_i(l)$ üres halmaz lenne. Legyen továbbá $S_i(l, v) = S_i(l) \cap A_i(v)$ és $S_i(l, u, v) = S_i(l) \cap A_i(u) \cap A_i(v)$ tetszőleges l egyenes és u, v pontok esetén. Hasonlóan, jelölje $\Omega_i(l) = \Omega_i \cap l$, $\Omega_i(l, v) = \Omega_i(l) \cap A'_i(v)$ és $\Omega_i(l, u, v) = \Omega_i(l) \cap A'_i(u) \cap A'_i(v)$.

Végül egy $\mathcal{A}$ eseményre jelölje szokásos módon $\mathbf{1}_{\mathcal{A}}$ az $\mathcal{A}$ indikátorát: $\mathbf{1}_{\mathcal{A}} = 1$, ha $\mathcal{A}$ teljesül és 0 különben. A logaritmusok mindvégig természetes alapúak.

3. fejezet

A fő tétel bizonyítása

Ebben a fejezetben kimondjuk a fő lemmánkat és ennek segítségével bebizonyítjuk az 1.2-es tételt. A fejezetet a fő lemma leírásával fogjuk kezdeni, azonban az egyes, lemmában szereplő tulajdonságok jobb megértéséhez a következő fejezetekre is szükség lesz.

3.1. A fő lemma

A fő lemmánk azt állítja, hogy bizonyos tulajdonságok 1 közeli valószínűséggel az algoritmus minden lépése során teljesülnek. Mint korábban már említettem, az algoritmus elemzéséhez azt két fázisra kell vágnunk, S_i méretétől függően. Az első fázis minden lépésében 3 elsődleges és 7 másodlagos tulajdonság teljesülésére kell ügyelnünk, a második fázisban 5 tulajdonságra. Mielőtt ezeket ismertetném, vezessünk be még egy jelölést: legyen $b'_i = \prod_{j=0}^{i-1}(1-P_j^l)$. Mivel $1-P_j^l$ felső becslés annak valószínűségére, hogy egy Ω_{j-1}-beli pont Ω_j-ben marad, b'_i nem más, mint annak az esélynek felső korlátja, hogy valamely fix Ω_0-beli pont Ω_i-ben marad. Legyenek továbbá, a korábbiakban már említettek szerint, $c = 300$ és $c_1 = 100$. Ezen paraméterek távolról sem ideálisak, de a konstansok optimalizálása egyelőre nem célunk. A tulajdonságok jobb megértéséhez az utánuk szereplő megjegyzés nyújt segítséget.

Első fázis

Ez a fázis mindazon lépésekből áll, ahol $b_i q$ legalább $\log^{c_1} q$. Ez nagyjából azt jelenti, hogy ebben a fázisban minden egyenesnek legalább $\log^{c_1} q$ túlélő pontja van (lásd lejjebb a második tulajdonságot). A következő tíz tulajdonságról szeretnénk, hogy a fázis minden lépésének outputjára teljesüljön:

Elsődleges tulajdonságok

(1) $\theta q^{1/2}(1-o(1)) \leq |M_i| \leq \theta q^{1/2}(1+o(1))$ és $|B_i| \leq 2\theta q^{1/2}$

(2) $b_{i+1}q(1-(i+1)\log^{-13} q) \leq |S_{i+1}(l)| \leq b_{i+1}q(1+(i+1)\log^{-13} q)$

(3) $|\Omega_{i+1}(l)| \leq b'_{i+1}q(1+(i+1)\log^{-13} q)$

Másodlagos tulajdonságok

Minden $u, v, w, z \in \Omega_i$ pontra és l egyenesre, melyre $l \cap \Omega_{i+1} \neq \emptyset$:

(4) $|S_{i+1}(l,v)| \leq 8(i+1)a_{i+1}b_{i+1}q^{1/2} + (i+1)\log^{40} q$

(5) $|S_{i+1}(l,u,v)| \leq (i+1)\log^4 q$

(6) $|A_{i+1}(u,v)| \leq (i+1)b_{i+1}q + (i+1)\log^{40} q$

(7) $|A_{i+1}(u,v,w)| \leq (i+1)b_{i+1}q^{1/2} + (i+1)\log^{22} q$

(8) $|A_{i+1}(u,v,w,z)| \leq (i+1)\log^6 q$

(9) $|\Omega_{i+1}(l,v)| \leq 8(i+1)a_{i+1}b'_{i+1}q^{1/2} + (i+1)\log^{40} q$

(10) $|\Omega_{i+1}(l,u,v)| \leq (i+1)\log^4 q$.

A korábban bevezetett jelölések közti kapcsolatot figyelembe véve igazak az alábbi összefüggések:

$$|T_{i+1}(v)| = \sum_{v\in l}\binom{|S_{i+1}(l)|-1}{2}, \quad |A_{i+1}(v)| = \sum_{l=(av),a\in A_{i+1}} (|S_{i+1}(l)|-1)$$

$$|S_{i+1}| = \sum_l |S_{i+1}(l)|/(q+1), \quad |\Omega_{i+1}| = \sum_l |\Omega_{i+1}(l)|/(q+1).$$

A **(2)**-es és **(3)**-as tulajdonságok, valamint a fenti átalakítások alapján a következő négy tulajdonságot írhatjuk fel:

(11) $\frac{1}{2}b_{i+1}^2 q^3(1-3(i+1)\log^{-13} q) \leq |T_{i+1}(v)| \leq \frac{1}{2}b_{i+1}^2 q^3(1+3(i+1)\log^{-13} q)$

(12) $a_{i+1}b_{i+1}q^{3/2}(1-2(i+1)\log^{-13} q) \leq |A_{i+1}(v)| \leq a_{i+1}b_{i+1}q^{3/2}(1+2(i+1)\log^{-13} q)$

(13) $(1-\log^{-10} q)^{i+1}b_{i+1}q^2 \leq |S_{i+1}| \leq (1+\log^{-10} q)^{i+1}b_{i+1}q^2$

(14) $|\Omega_{i+1}| \leq (1+\log^{-10} q)^{i+1}q^2 b'_{i+1}$

A második fázis során ezt a négy tulajdonságot szeretnénk teljesíteni (egy kicsit más hibataggal a **(12)**-esben) az **(1)**-essel együtt.

Második fázis

A második fázis mindazon $i+1$ lépésekből áll, mely inputjára teljesül:

$$q^{-3/2}\log^c q \leq b_i \leq q^{-1}\log^{c_1} q.$$

Az első fázis **(2)**-es tulajdonságából fakadóan a második fázis akkor indul, amikor minden egyenesnek nagyjából $\log^{c_1} q$ túlélő pontja van. A szükséges tulajdonságok a következők (minden $v \in \Omega_{i+1}$ pontra):

(1) $\theta q^{1/2}(1-o(1)) \le |M_i| \le \theta q^{1/2}$ és $|B_i| \le 2\theta q^{1/2}(+o(1))$

(2) $\frac{1}{2}b_{i+1}^2 q^3(1-3(i+1)\log^{-13} q) \le |T_{i+1}(v)| \le \frac{1}{2}b_{i+1}^2 q^3(1+3(i+1)\log^{-13} q)$

(3) $a_{i+1}b_{i+1}q^{3/2}(1-O(i\theta^2)) \le |A_{i+1}(v)| \le a_{i+1}b_{i+1}q^{3/2}(1+O(i\theta^2))$

(4) $(1-\log^{-10} q)^{i+1}b_{i+1}q^2 \le |S_{i+1}| \le (1+\log^{-10} q)^{i+1}b_{i+1}q^2$

(5) $|\Omega_{i+1}| \le (1+\log^{-10} q)^{i+1}q^2 b'_{i+1}$

Azt mondjuk, hogy az algoritmus *tökéletesen* fut a j-edik lépésig, ha a megkövetelt tulajdonságok teljesülnek az $1, 2, \ldots, j$ lépések outputjaira. Ha mindkét fázis valamennyi lépésénél az összes tulajdonság teljesül, azt mondjuk, hogy az algoritmus *teljesen tökéletesen* fut.

Megjegyzés:

- Az i+1-edik lépés előtt S_i-nek nagyjából $b_i q^2$ pontja van (emlékeztetőül: b_i alsó korlát annak valószínűségére, hogy egy tetszőleges Ω_0-beli pont S_i-ben marad). Ebben a lépésben S_i tetszőleges pontját $p_i = \theta(b_i q^{3/2})^{-1}$ valószínűséggel választjuk be B_i-be, így tehát B_i-nek nagyjából $b_i q^2 p_i = b_i q^2 \theta (b_i q^{3/2})^{-1} = \theta q^{1/2}$ pontja van. Mivel az ütközéseket okozó pontok száma kicsi, B_i legtöbb pontja M_i-ben is megmarad. Így M_i elemszámát is körülbelül $\theta q^{1/2}$-nek várhatjuk, ez jelenik meg mindkét fázis első tulajdonságában.

- Az első fázis **(2)**-es és a második fázis **(2-4)**-es tulajdonságaiban a jobb és bal oldalon szereplő fő tagok épp a vizsgált mennyiségek várható értékei. Így ezen tulajdonságok voltaképp azt állítják, hogy a kérdéses mennyiségek erősen koncentráltak a várható értékeik körül.

- Ahogy nemsokára látni fogjuk, az 1.2-es tétel bizonyítása (melyhez a fő lemmát használjuk) csupán a tulajdonságok egy kis részét igényli (például a másodlagos tulajdonságok egyikét sem fogjuk használni). Sajnos azonban az elsődleges tulajdonságok önmagukban indukcióval nem bizonyíthatók. A másodlagosakat pontosan azért vezetjük be, mert az elsődleges tulajdonságokkal együtt már egy kellőképpen erős indukciós hipotézist szolgáltatnak, amit be tudunk bizonyítani. A fejezet végén szereplő megjegyzés még tisztább képet ad majd a fenti mennyiségek közti kapcsolatról.

3.1. Lemma (Fő lemma) *Az algoritmus 1 közeli valószínűséggel teljesen tökéletesen fut.*

A következő két szakaszban belátjuk, hogy ha az algoritmus teljesen tökéletesen fut, akkor a végső A_N ív teljesíti az 1.2-es tétel állítását.

3.2. További lemmák

Ebben a részben az 1.2-es tétel bizonyításához szükséges becsléseket vizsgálunk. A kulcs tényező, ahova szeretnénk eljutni, a következő: ha az algoritmus teljesen tökéletesen fut, akkor a $P_i^u - P_i^l$ rés minden lépésben kellően kicsi. Mivel $|\Omega_0|\prod_{i=0}^{N-1}(1-P_i^l)$ alapvetően $|\Omega_N|$ felső becslése és $|\Omega_0|\prod_{i=0}^{N-1}(1-P_i^u)$ alsó becslés $|S_N|$-re, a $P_i^u - P_i^l$-ekre vonatkozó megfelelő korlátokból következni fog, hogy $|\Omega_N|/|S_N| = O(1)$. Másrészt a megállási idő és a második fázis **(4)**-es tulajdonságából $|S_N| = O(q^{1/2}\log^c q)$, így kapjuk $|\Omega_N|$-re is az $O(q^{1/2}\log^c q)$-s korlátot. Ahogy azonban korábban már láttuk, a szelőkkel még nem fedett pontok halmaza $\Omega_N \bigcup(\cup_{i=1}^N B_i \setminus M_i)$ részhalmaza, az unió második tagjának hozzájárulása viszont – köszönhetően annak, hogy kevés pontot választunk ki, és így kevés okoz ütközést – elenyésző $|\Omega_N|$ mellett.

Az első két lemma felső, illetve alsó korlátot ad a P_i^u, valamint P_i^l mennyiségekre. A korlátok egyben azt is megmagyarázzák, hogy miért van szükség a fő lemmában az $|A_i(v)|$ és $|T_i(v)|$-re vonatkozó becslésekre.

3.2. Lemma

$$P_i^u \le p_i + p_i \max_v |A_i(v)| + p_i^2 \max_v |T_i(v)|,$$

ahol a maximumot az Ω_i halmazon vesszük.

Bizonyítás: Tudjuk (a törlés definíciójából), hogy a következő három oka van annak, ha egy $v \in \Omega_i$ pontot törlünk:

$$P_i(v) \le P(v \in B_i) + P(B_i \cap A_i(v) \neq \emptyset) + P(\exists l : v \in l \text{ és } |B_i \cap (l \setminus v)| \ge 2).$$

Jelölje P_1 a jobboldal első, P_2 a második, P_3 a harmadik tagját. Nyilvánvaló, hogy $P_1 \le p_i$ (ha v nincs benne S_i-ben, a szigorú egyenlőtlenség is lehetséges). Belátjuk, hogy $P_2 \le p_i \max|A_i(v)|$, ehhez:

$$P_2 = 1 - P(B_i \cap A_i(v) = \emptyset) = 1 - (1-p_i)^{|A_i(v)|} \le 1 - (1 - p_i|A_i(v)|) = p_i|A_i(v)|.$$

(Az utolsó előtti lépésben a Bernoulli-egyenlőtlenséget használtuk.) Végül P_3 fölső becsléséhez vegyük észre, hogy

$$P_3 \le p_i^2 \sum_{v\in l} \binom{|l\setminus v|}{2} \le p_i^2 \max_v |T_i(v)|.$$

Ezzel beláttuk az állítást. ■

3.3. Lemma

$$P_i^l \ge p_i \min_v |A_i(v)| - 2p_i^2 \max_v |A_i(v)|^2 - p_i^3 \max_v |A_i(v)| \max_v |T_i(v)|,$$

a maximumot és a minimumot az Ω_i halmazon véve.

Bizonyítás: Vegyük észre (ismét az egyik törlések alapján), hogy

$$P_i(v) \geq P(M_i \cap A_i(v) \neq \emptyset) = 1 - P(M_i \cap A_i(v) = \emptyset).$$

$P(M_i \cap A_i(v) = \emptyset)$ felső becsléséhez bontsuk szét az eseményt két részre:

$$P(M_i \cap A_i(v) = \emptyset) = P(B_i \cap A_i(v) = \emptyset) + P(\{B_i \cap A_i(v) \neq \emptyset\} \wedge \{M_i \cap A_i(v) = \emptyset\}) = P_4 + P_5,$$

ahol P_4 és P_5 a jobboldal első, illetve második tagját jelöli. Az előző bizonyításhoz hasonlóan:

$$P_4 = (1-p_i)^{|A_i(v)|} \leq 1 - p_i|A_i(v)| + p_i^2 \binom{|A_i(v)|}{2} \leq 1 - p_i \min_v |A_i(v)| + p_i^2 \max_v \binom{|A_i(v)|}{2},$$

továbbá

$$P_5 \leq \sum_{x \in A_i(v)} P(\{x \in B_i\} \wedge \{x \notin M_i\}) \leq |A_i(v)| \max_{x \in A_i(v)} P(\{x \in B_i\} \wedge \{x \notin M_i\}) \leq$$

$$\leq |A_i(v)| p_i \max_{x \in A_i(v)} (P(B_i \cap A_i(x) \neq \emptyset) + P(\exists l : x \in l \text{ és } |B_i \cap (l \setminus x)| \geq 2)) \leq$$

$$\leq |A_i(v)| p_i \max_{x \in A_i(v)} (p_i |A_i(x)| + p_i^2 |T_i(x)|)$$

(a második sor felírásához felhasználtuk, hogy miket neveztünk jó pontoknak, lásd az algoritmus leírásánál). A lemma állítása P_4 és P_5 becsléséből már következik. ■

3.4. Megjegyzés A későbbiek során (feltéve, hogy az algoritmus az i-edik lépésig tökéletesen fut) gyakran fogunk hivatkozni a következő aszimptotikus egyenlőségekre:

$$p_i |A_i(v)| \sim \theta (b_i q^{3/2})^{-1} a_i b_i q^{3/2} = \theta a_i \sim i\theta^2$$

(az utolsó átalakítás során felhasználtuk, hogy $a_i = |A_i| q^{-1/2}$, továbbá tudjuk, hogy A_i az M_i-kből tevődik össze, melyeknek minden lépésben nagyjából $\theta q^{1/2}$ pontja van).

$$p_i^3 |A_i(v)||T_i(v)| \sim \frac{1}{2}\theta^3 a_i \sim \frac{1}{2} i\theta^4$$

$$p_i^2 |T_i(v)| \sim \frac{1}{2}\theta^2$$

$A \sim B$ alatt azt értjük, hogy A/B egy közeli, de a számításokhoz általában csak $0,9 \leq A/B \leq 1,1$-re lesz szükségünk.

A következő lemmában a futási időre adunk becslést:

3.5. Lemma *Ha az algoritmus teljesen tökéletesen fut, a futási idő* $N = \Theta(\theta^{-1} \log^{1/2} q)$.

Bizonyítás: N definíciójából következik, hogy

$$\prod_{i=0}^{N-1} (1 - P_i^u) = b_N \leq q^{-3/2} \log^c q \leq b_{N-1} = \prod_{i=0}^{N-2} (1 - P_i^u).$$

Indirekt tegyük fel, hogy $N \geq L = 10\theta^{-1}\log^{1/2} q$ (az egyszerűség kedvéért az is feltehető, hogy L egész szám). Az $i \mapsto b_i$ függvény monoton fogyásából következik, hogy

$$b_L \geq b_{N-1} \geq q^{-3/2}\log^c q. \tag{3.1}$$

Másrészt definíció szerint

$$b_L = \prod_{i=0}^{L-1}(1-P_i^u) \leq \prod_{i=0}^{L-1}(1-P_i^l).$$

Az egyenlőtlenség mindkét oldalából logaritmust véve, a 3.1-es alapján

$$-(\frac{3}{2}+o(1))\log q \leq \sum_{i=0}^{L-1}\log(1-P_i^l).$$

A jobboldal becsléséhez a 3.3-as lemmát használjuk. Nyilvánvaló, hogy ha az algoritmus teljesen tökéletesen fut, akkor P_i^l alsó becslésében a $p_i|A_i(v)|$ tag fog dominálni (lásd a 3.4-es megjegyzést). Mivel $i \leq L-1$, $i\theta^2 = o(1)$ (emlékeztetőül, $\theta = \log^{-2} q$). Így a 3.4-es megjegyzés alapján $P_i^l \geq \frac{1}{2}i\theta^2$, és ezért

$$\log(1-P_i^l) \leq \log(1-\frac{1}{2}i\theta^2) \leq -\frac{1}{4}i\theta^2.$$

Ebből

$$\sum_{i=0}^{L-1}\log(1-P_i^l) \leq -\frac{1}{4}\sum_{i=0}^{L-1} i\theta^2 \leq -\frac{1}{10}L^2\theta^2 = -10\theta^{-2}\log q\theta^2 \leq -2\log q,$$

ami ellentmond a 3.1-esből levont következtetésünknek. Így $N \leq L = 10\theta^{-1}\log^{1/2} q$. Hasonló gondolatmenettel, P_i^u becslését használva belátható, hogy $N \geq \frac{1}{10}\theta^{-1}\log^{1/2} q$, és ezzel bebizonyítottuk a lemmát. ■

Megjegyzés: Vegyük észre, hogy a 3.5-ös lemma bizonyításában N felső becsléséhez nem használtuk ki, hogy az algoritmus teljesen tökéletesen fut, csupán arra van szükségünk, hogy az i-edik lépésig tökéletesen fusson minden $i \leq L-1$-re. Ezért a későbbi indukciós bizonyításokban, ahol az indukció alapja az lesz, hogy az algoritmus az i-edik lépésig tökéletesen fut, felhasználhatjuk, hogy a lépésszám legfeljebb N, azaz $i \ll \log^3 q$. Az N-re vonatkozó alsó becslés egyébként sem kritikus, mivel nincs szükségünk az 1.1-es tételben szereplő ív méretének alsó korlátjára, csupán az 1.4-es következmény igazolásához hasznos.

Az előző lemma és $|M_i|$ mindkét fázisbeli becsléséből (lásd az **(1)**-es tulajdonságokat) könnyen kiszámolható:

3.6. Következmény *Ha az algoritmus teljesen tökéletesen fut, akkor*

$$|A_N| = \Theta(q^{1/2}\log^{1/2} q).$$

A szakasz utolsó lépéseként belátjuk a kulcs tényezőt, miszerint $P_i^u - P_i^l$ minden i-re kellően kicsi.

3.7. Lemma *Ha az algoritmus teljesen tökéletesen fut, akkor minden i-re*

$$P_i^u - P_i^l = O(\theta^2 \log q) = O(\log^{-1} q).$$

Bizonyítás: A 3.2-es és 3.3-as lemmákból következik, hogy

$$P_i^u - P_i^l \le p_i(1 + \max_v |A_i(v)| - \min_v |A_i(v)|) + p_i^2 \max_v |T_i(v)| + 2p_i^2 \max_v |A_i(v)|^2 + \\ + p_i^3 \max_v |A_i(v)| \max_v |T_i(v)|. \tag{3.2}$$

$|T_i(v)|$ fő lemmában szereplő becslése ($|T_i(v)| \sim \frac{1}{2} b_i^2 q^3$) miatt $p_i^2 \max_v |T_i(v)| = O(\theta^2)$ (vö. a 3.4-es megjegyzéssel). Felhasználva (ismét csak a fő lemmából), hogy $|A_i(v)| \sim a_i b_i q^{3/2}$, kapjuk, hogy $p_i^3 \max_v |A_i(v)| \max_v |T_i(v)| = O(a_i \theta^3) = o(\theta^2 \log q)$ – lévén a 3.6-os megjegyzés alapján $a_i = O(\log^{1/2} q)$ (jusson eszünkbe, hogy $a_i = |A_i|/q^{1/2} \le |A_N|/q^{1/2}$). Továbbá $p_i^2 \max_v |A_i(v)|^2 \sim a_i^2 \theta^2 = O(\theta^2 \log q)$. Így már csak azt kell megmutatni, hogy $p_i(\max_v |A_i(v)| - \min_v |A_i(v)|) = O(\theta^2 \log q)$.

A fő lemma becslései szerint $p_i(\max_v |A_i(v)| - \min_v |A_i(v)|)$ értéke a második fázisban nagyobb (ebben a fázisban ugyanis az $|A_i(v)|$-re vonatkozó hibatag nagyobb, mint az elsőben), mégpedig a **(3)**-as tulajdonság szerint

$$\max_v |A_i(v)| - \min_v |A_i(v)| = O(i\theta^2 a_i b_i q^{3/2}).$$

Mivel $p_i = \theta(b_i q^{3/2})^{-1}$, ezért

$$p_i(\max_v |A_i(v)| - \min_v |A_i(v)|) = O(i a_i \theta^3). \tag{3.3}$$

Másrészt $a_i \le a_N = \Theta(\log^{1/2} q)$ és $i \le N = O(\theta^{-1} \log^{1/2} q)$. A 3.3-asból és ezekből együttesen már következik a lemma állítása. ■

3.3. Az 1.2-es tétel bizonyítása

Ebben a szakaszban megmutatjuk, hogy ha az algoritmus teljesen tökéletesen fut, akkor az outputra a következő három becslés teljesül: $|A_N| = \Theta(q^{1/2} \log^{1/2} q)$, $|\Omega_N| = O(q^{1/2} \log^c q)$ és $|\cup_{i=1}^N B_i \setminus M_i| = O(q^{1/2} \log^{1/2} q)$. Ahogy korábban már említettük, az algoritmus leállása után fedetlenül maradt pontok halmaza $\Omega_N \bigcup (\cup_{i=1}^N B_i \setminus M_i)$ részhalmazát képezi, így ezekből a becslésekből már megkapjuk a tétel állítását.

Az első becslés már a 3.6-os következményben szerepelt. A második becsléshez vegyük észre, hogy a megállási idő definíciójából, valamint a második fázis **(4)**-es tulajdonságából fakadóan $|S_N| \le q^{1/2} \log^c q$. Így elég belátni, hogy $|\Omega_N|/|S_N| = O(1)$. Valójában még több is igaz: $|\Omega_N|/|S_N| = 1 + o(1)$. Ehhez az első fázis **(14)**-es és a második fázis **(5)**-ös tulajdonsága alapján írjuk fel:

$$|\Omega_N| \le (1 + \log^{-10} q)^N b'_N q^2 = (1 + o(1)) b'_N q^2 = (1 + o(1)) \prod_{i=0}^{N-1} (1 - P_i^l) q^2.$$

Másrészt $|S_N| = (1+o(1))b_N q^2 = (1+o(1))\prod_{i=0}^{N-1}(1-P_i^u)q^2$. Ezért

$$|\Omega_N|/|S_N| = (1+o(1))\left(\prod_{i=0}^{N-1}\frac{1-P_i^l}{1-P_i^u}\right). \tag{3.4}$$

Ugyanakkor a 3.7-es lemma alapján

$$\log\frac{1-P_i^l}{1-P_i^u} = O(P_i^u - P_i^l) = O(\theta^2\log q).$$

Végül használjuk fel, hogy $\theta = \log^{-2} q$ és a 3.5-ös lemma alapján $N = \Theta(\theta^{-1}\log^{1/2} q)$, így

$$\log\frac{|\Omega_N|}{|S_N|} = O(N\theta^2\log q) = O(\theta\log^{3/2} q) = o(1).$$

A harmadik becslésünk triviális következménye az N-re, valamint a $|B_i|$-re vonatkozó felső korlátoknak (ez utóbbit lásd mindkét fázis első tulajdonságának második felében). ■

3.8. Megjegyzés A későbbiekben (feltéve, hogy az algoritmus az i-edik lépésig tökéletesen fut) gyakran fogjuk használni a következőket:

$$a_i\theta \sim i\theta^2 \le N\theta^2 = O(\log^{1/2} q\theta) = o(1) \qquad a_i \sim i\theta = O(\log^{1/2} q) = o(\log q).$$

A 3.2-es lemmából (és a 3.4-es megjegyzésből) pedig következik, hogy $P_i^u = o(1)$. Másrészt $b_{i+1} = b_i(1-P_i^u)$, ezért a fenti feltételezés mellett $b_{i+1} \sim b_i \ge 0,9b_i$.

Megjegyzés: Láthattuk, hogy az 1.2-es tétel bizonyításában közvetlenül is megjelentek az $|A_i(v)|, |T_i(v)|, |M_i|, |S_i|, |\Omega_i|$ mennyiségek, ez magyarázza, hogy miért van szükség a fő lemmában az ezekre vonatkozó becslésekre. Ahhoz, hogy az első fázisban $|A_i(v)|, |T_i(v)|$ és $|S_i|$ értékét kordában tudjuk tartani, $|S_i(l)|$ értékének kontrollálására van szükségünk minden l esetén (lásd a kettes tulajdonságot). Ez azért lehetséges, mert ebben a fázisban $|S_i(l)|$ kellően nagy ($|S_i(l)| \ge \log^{c_1} q$), és ennek segítségével belátható, hogy az $|S_i(l)|$-ek, mint valószínűségi változók, erősen koncentráltak. Az első fázis **(4-5)**-ös tulajdonságait azért vezettük be, hogy $|S_i(l)|$ értékét szabályozhassuk (ennek kifejtését lásd az ötödik fejezetben). A második fázisban azonban $|S_i(l)|$ nagyon kis értékeket is felvehet, ezért a koncentráció ebben a fázisban nem teljesül. Emiatt $|A_i(v)|, |T_i(v)|$ és $|S_i|$ értékét közvetlenül kell kezelni. Ahhoz, hogy $|A_i(v)|$-t ebben a fázisban korlátozni tudjuk, már az első fázisban előkészületekre van szükség, ezt célozza a **(6)**-os tulajdonság, együttesen a **(7-8)**-assal, melyekre a **(6)**-os bizonyításához lesz szükségünk. Végül, hasonlóan $|S_i|$ esetéhez, ahhoz, hogy $|\Omega_i|$ értékét az első fázisban kontrollálhassuk, $|\Omega_i(l)|$ korlátozására van szükségünk, ehhez vezettük be a **(3)**-as, **(9)**-es és **(10)**-es tulajdonságokat.

4. fejezet

A koncentráció kérdése

Sok véletlen módszeren alapuló bizonyítás központi eleme bizonyos valószínűségi változók várható érték körüli koncentrációja. Mit is értünk azonban „erős koncentráción”? Egy tipikus ilyen eredmény Chernoff következő tétele:

4.1. Tétel *Legyen* $Y = \sum_{i=1}^{n} t_i$, *ahol a* t_i*-k független azonos eloszlású bináris véletlen változók* p *várható értékkel. Ekkor tetszőleges* $\lambda > 0$*-ra*

$$P(|Y - E(Y)| \geq \sqrt{\lambda n}) \leq 2e^{-\lambda/2}.$$

Azt mondjuk, hogy egy függvény erősen koncentrált, ha egy Chernoff-típusú exponenciális szóráskorlát teljesül rá. A matematika számos területén alapvető fontossággal bír a kérdés, hogy vajon egy függvény erősen koncetrált-e vagy sem. A problémát évszázadok óta jelentős matematikusok kutatják, a legfigyelemreméltóbb eredmények nagyszerű összefoglalóját adja M. Talagrand műve [11] a témából.
A koncentráció elméletének középpontjában a következő jelenség áll:

Ha Y *egyenletesen simán függ a* $t_1, \ldots, t_n$ *változóktól, akkor* Y *erősen koncentrált.* (4)
A simaságot tradicionálisan a Lipschitz-együtthatóval definiálják. Ennek értelmében egy $Y = Y(t_1, \ldots, t_n)$ Ω-ból (Ω a t_i-k által kifeszített szorzattér a természetes szorzatmértékkel tekintve) $\mathbb{R}$-be képező függvényt r-*lipschitzes*nek nevezünk, ha r az a legkisebb szám, hogy valamennyiszer két n-dimenziós bináris vektor, t és t' csak egyetlen koordinátában tér el, $|Y(t) - Y(t')| \leq r$. Azt mondjuk, hogy Y sima, ha r – n-hez és Y várható értékéhez viszonyítva – relatíve kicsi. A következő, úgynevezett Azuma-egyenlőtlenség kiválóan illusztrálja a (4)-es jelenséget:

4.2. Tétel *Ha* Y *Lipschitz-együtthatója* r*, akkor tetszőleges* $\lambda > 0$ *számra*

$$P(|Y - E(Y)| \geq r\sqrt{\lambda n}) \leq 2e^{-\lambda/2}.$$

Hasonló eredményt ad a Talagrand-egyenlőtlenség is.

Abban az esetben, ha az r Lipschitz-együttható kicsi, Azuma és Talagrand egyenlőtlenségei tökéletes eszközök. Ahogy azonban r nő, ezen egyenlőtlenségek egyre kevésbé hatékonyak. Képzeljük el például azt a tipikus szituációt, mikor a farok nagyságrendje $O(E(Y))$. Ekkor a fentebb bemutatott Azuma-egyenlőtlenség $r \gg \sqrt{E(Y)}$ esetén már csak triviális korlátot képes adni. Sajnos azonban számos probléma során, így szakdolgozatom későbbi részeiben is, nagy Lipschitz-együtthatójú függvényekkel kell foglalkoznunk. Ennek igazolásához tekintsük a következő példát: vizsgáljuk M_1 méretét. Minden $x \in S_0$ esetén legyen $t_x = 1$, ha x-et kiválasztottuk B_1-be, és 0 különben. Így $|M_1|$ a $t_x, x \in S_0$ atomoktól függő véletlen változó. Megmutatjuk, hogy a legrosszabb esetben M_1 Lipschitz-együtthatója még $\Omega(q)$ nagyságrendű is lehet. Ehhez tegyük fel, hogy a Galois-síkon vagyunk, és legyen $\mathcal{C}$ az $xy = z^2$ egyenletű kúpszelet. Könnyen látható, hogy $\mathcal{C}$ egy ív. Egy $v \in S_0$ pontra jelölje $l_1, \ldots, l_{q+1}$ a v-re illeszkedő egyeneseket, körülbelül a fele ezen egyeneseknek pontosan két pontban metszi $\mathcal{C}$-t. Jelöljük ezen pontpárokat $(x_1, y_1), \ldots, (x_K, y_K)$-val, ahol $K \approx q/2$. Képzeljük el, hogy a kiválasztás műveleténél v kivételével minden pont szóba jöhet, és a lehetséges pontok közül az összes (x_i, y_i)-t $(i = 1, \ldots, K)$ kiválasztottuk, de semmi mást. Ekkor v választásának nagy hatása van $|M_1|$-re: ha v-t kiválasztjuk, az megöli az egész konstrukciót, és így $|M_1| = 0$, míg ha v-t nem választjuk ki, akkor $M_1 = \{x_1, y_1, \ldots, x_K, y_K\}$ és $|M_1| \approx q$.

Egy másik tipikus példa nagy Lipschitz-együtthatójú függvényre a következő jól ismert probléma a véletlen gráfok elméletéből (a fejezet során később ugyanezen a példán fogom illusztrálni a Kim–Vu szerzőpáros által kidolgozott új koncentrációs eredmény erejét is): a $G(N, p)$ véletlen gráfot N csúcson úgy definiáljuk, hogy tetszőleges $ij, 1 \leq i < j \leq N$ élt egymástól függetlenül p valószínűséggel húzunk be, ahol p általában N függvénye szokott lenni. Ebben az esetben $n = \binom{N}{2}$ független azonos eloszlású t_{ij} véletlen változónk van, melyek a választásainkat reprezentálják: $t_{ij} = 1$, ha az ij élt behúztuk, és 0 különben. Azt mondjuk, hogy három csúcs, i, j és k háromszöget alkot, ha bármely kettő között vezet él. Jelölje Y a háromszögek számát $G(N, p)$-ben. Exponenciális korlátot szeretnénk kapni a következő valószínűségre:

$$P(|Y - E(Y)| \geq \epsilon E(Y)), \tag{4.1}$$

ahol ϵ egy fix pozitív konstans és p kellően kicsi.
Tegyük fel például, hogy $p = \Theta(N^{-3/4})$. Ekkor $E(Y) = \binom{N}{3}p^3 = \Theta(N^{3/4})$. Mivel egy élt $N - 2$ háromszög tartalmazhat, egyetlen él törlése akár $N - 2$-vel is megváltoztathatja Y értékét. Így Y Lipschitz-együtthatója legalább $N - 2$ (valójában pontosan $N - 2$), ami jóval nagyobb, mint $E(Y)$, így az Azuma-egyenlőtlenség nem ad nemtriviális korlátot.

Láthatjuk tehát, hogy ebben az esetben Y a hagyományos értelemben nem nevezhető simának. Azonban igen ritka esemény, hogy egyetlen él $N - 2$ háromszöget feszítsen. Egy rögzített e élre az általa feszített háromszögek várható értéke csupán $(N-2)p^2 = O(1)$. Ez arra mutat, hogy ahhoz, hogy erős koncentrációs eredményt kaphassunk, a legrosszabb eset

Lipschitz-együtthatója helyett inkább átlagos vagy tipikus Lipschitz-együtthatóra lenne szükségünk. A simaság szempontjából megközelítve a kérdést, egyfajta átlagos simasággal szeretnénk dolgozni a (4)-esben definiált globális simaság helyett. Igen fontos tehát olyan értelmes definíciót találnunk az átlagos simaságra, hogy függvények nagy osztályára a (4)-es következő variációja teljesüljön:

Ha Y átlagban sima, akkor erősen koncentrált.

Az általánosság legmagasabb szintjén lehetetlennek tűnik ilyen definíciót alkotni, de a diszkrét problémák esetén a függvényeknek többnyire speciális felépítése van, ami lehetővé teszi számunkra, hogy egy további indukciós érvelést alkalmazhassunk az elemi változók számától eltérő paraméteren is (mind az Azuma-, mind a Talagrand-egyenlőtlenség igazolása az elemi változók számán alapuló indukcióval történik).

4.1. Általános megközelítés

Első lépésként approximálni fogjuk az Y függvényünket. Egy $t \in \Omega$ pontot *jó*nak nevezünk, ha t bármely koordinátájának megváltoztatása nem befolyásolja (egy bizonyos értelemben) túlságosan Y-t. Minden egyéb pont *rossz*. A lépés során Y-t egy olyan Y' függvénnyel akarjuk közelíteni, hogy

(∗) $E(Y) = E(Y')$,

(∗∗) Y' erősen koncentrált,

(∗ ∗ ∗) $Y(t) = Y'(t)$ minden jó t pontra.

A rossz tartomány kivágása (mely a nagy Lipschitz-együtthatójú rossz pontokból áll) teljesen természetes megközelítés. A kritikus pont az érvelésünkben az, hogy a rossz pontok halmazát úgy definiáltuk, hogy az nemcsak Y' erős koncentrációját biztosítja, hanem lehetőséget ad a második lépés során indukciós érvelés használatára is.
A bizonyítás során igen kényelmesnek tűnik az is, hogy $E(Y) = E(Y')$. (A gyakorlatban többnyire az is elég, ha garantálni tudjuk, hogy $|E(Y)-E(Y')|$ sokkal kisebb, mint Y farok eltérése.)

A második lépésben ki kell használnunk Y felépítését. Tegyük fel például, hogy Y egy k-fokú polinom (esetünkben valóban ilyen polinomokról lesz szó). Ha megvan a kívánt Y' közelítő függvény, a következőképpen haladhatunk tovább: mivel Y és Y' várható értéke megegyezik, ezért

$$P(|Y - E(Y)| \geq T) \leq P(|Y' - E(Y')| \geq T) + P(Y \neq Y').$$

A (∗∗) miatt Y' már erősen koncentrált, így csak a $P(Y \neq Y')$ valószínűséget kell becsülnünk. Ehhez a (∗∗∗)-as feltételt kihasználva csak a rossz halmaz mértékét kell korlátoznunk.

Ezt a halmazt azonban az előző lépésben kellő előrelátással hoztuk létre, így mértékét más polinomok nagy szórási valószínűségeinek összegével becsülhetjük. Ezek a polinomok Y elsőrendű parciális deriváltjaiból származnak és legfeljebb $k-1$-fokúak. Ennek a kritikus ténynek a segítségével tudunk indukciót alkalmazni a fokszámon, hogy a kérdéses nagy szórási valószínűségeket behatárolhassuk. A parciális deriváltak megjelenése nem jelent nagy meglepetést, hisz maga Y Lipschitz-együtthatója is tekinthető az elsőrendű parciális deriváltak maximumértékének.

Az egész megközelítés központi eleme magának a tételnek a megfogalmazása volt. Kiderült, hogy valóban lehetséges a globális helyett az átlagos Lipschitz-együtthatót használó hipotézis felállítása, ezt megtalálni viszont igen nehéznek bizonyult. A megfelelő indukciós hipotézis azonban nemcsak egy erős eredményhez vezetett, hanem a fő lemmánk bizonyítását is leginkább bizonyos feltételek rutinellenőrzésére redukálta, ahogyan azt az 5. fejezetben látni fogjuk.

A következő két szakaszban ezt a fenti elven működő új koncentrációs eredményt fogom – bizonyítás nélkül – bemutatni (a lemmák bizonyítása a szerzőpáros *Concentration of multivariate polynomials and its applications* [6] című cikkében található), egyben megnevezve az esetünkben szükséges rossz tartományt is. Megjegyzendő, hogy a nagy (globális) Lipschitz-együttható okozta problémán akkor is felül tudunk kerekedni, ha a Lipschitz-együtthatók négyzetösszege nem túl nagy, a következőkben ez az eset is szerepet játszik majd.

4.2. Martingálok

Ebben a szakaszban ismét szükségünk lesz egy n független, kétértékű véletlen változó, $t_1, \ldots, t_n$ által generált valószínűségi mezőre a szorzatmértékkel ellátva. Ehhez jelölje p_i t_i várható értékét. Az aszimptotikus jelöléseink $n \to \infty$ mellett értendők.

Legyen Y $t_1, \ldots, t_n$ függvénye. Tetszőleges $v = (t_1, \ldots, t_n)$ vektorra és $1 \leq i \leq n$-re definiáljuk a következő $C_i(v)$ mennyiséget (ez szerepel majd átlagos Lipschitz-együtthatóként): jelölje $v^{(1)}$, illetve $v^{(0)}$ azon vektorokat, melyeket úgy kapunk v-ből, hogy az i-edik koordinátáját 1-nek, illetve 0-nak rögzítjük, ekkor

$$C_i(v) = \left| E\left(Y(v^{(1)}) - Y(v^{(0)}) | t_1, \ldots, t_{i-1}\right)\right|.$$

$C_i(v)$ a t_i véletlen változó *(feltételes) átlagos hatása*, ha $t_1, \ldots, t_{i-1}$ adott. Definíció szerint $C_i(v)$ $t_1, \ldots, t_{i-1}$ és $p_{i+1}, \ldots, p_n$ függvénye. A megfelelő *(feltételes) szórásnégyzet korlát*, $p_i C_i(v)^2$ is fontos szerepet játszik majd (ezek összege veszi át a Lipschitz-együtthatók négyzetösszegének szerepét), ennek pontos bevezetését lásd [6] 422. oldalán.

Ahogy korábban említettük, a klasszikus Azuma-típusú koncentrációs egyenlőtlenségek esetünkben nem alkalmazhatók, helyette szükségünk lesz egy kis valószínűségű rossz eset kizárására, hogy az átlagos esetekkel dolgozhassunk. Mivel azt szeretnénk, hogy minden

átlagos $C_i(v)$ hatás és a szórásnégyzet korlátok összege elég kicsi legyen, definiáljuk a rossz esetet a következőképpen:

$$\mathbb{B}_0 = \mathbb{B}_0(\mathbf{C}, \mathbf{V}) = \{v \mid \max_i C_i(v) \geq \mathbf{C} \text{ vagy } \sum_i p_i C_i(v)^2 \geq \mathbf{V}\}. \tag{4.2}$$

Néha kényelmesebb lesz ezt a következő formában felírni:

$$\mathbb{B}_1 = \mathbb{B}_1(\mathbf{C}, \mathbf{V}) = \{v \mid \max_i C_i(v) \geq \mathbf{C} \text{ vagy } \sum_i p_i C_i(v) \geq \mathbf{V}/\mathbf{C}\}.$$

Mivel $\sum_i p_i C_i(v)^2 \leq \max_i C_i(v) \sum_i p_i C_i(v)$, ezért $\mathbb{B}_0 \subseteq \mathbb{B}_1$.

4.3. Lemma *Tetszőleges $\lambda, \mathbf{C}$ és $\mathbf{V}$ pozitív számokra, melyekre $0 \leq \lambda \leq \mathbf{V}/\mathbf{C}^2$:*

$$P\left(|Y - E(Y)| \geq (\lambda \mathbf{V})^{1/2}\right) \leq 2e^{-\lambda/4} + P(\mathbb{B}_0).$$

Azaz

$$P\left(|Y - E(Y)| \geq (\lambda \mathbf{V})^{1/2}\right) \leq 2e^{-\lambda/4} + P(\mathbb{B}_1).$$

A lemma alkalmazásához természetesen szükségünk van a $\mathbf{C}$ és $\mathbf{V}$ (döntő) paraméterek megfelelő választására, erről a 4.4-es és 4.5-ös szakaszokban lesz szó.

4.3. Polinomok koncentrációja

Legyen H egy $\mathcal{V}(H) = \{1, 2, \ldots, n\}$ csúcshalmazú hipergráf, élhalmazát jelölje $\mathcal{E}(H)$ (az üres éleket is megengedjük). Tegyük fel, hogy minden e élnek legfeljebb k csúcsa lehet, és minden élhez rendeljünk hozzá egy pozitív $w(e)$ súlyt. Legyenek $t_i, i = 1, 2, \ldots, n$ független valószínűségi változók, ahol t_i vagy p_i várható értékű kétértékű változó, vagy $t_i = p_i$ 1 valószínűséggel. Tekintsük a következő függvényt:

$$Y_H = \sum_{e \in \mathcal{E}(H)} w(e) \prod_{s \in e} t_s.$$

Ezt a H-t az $Y = Y_H$ *támaszhipergráf*jának nevezzük. Vegyük észre, hogy Y egy legfeljebb k-fokú polinom. Ha e üres él, legyen $\prod_{s \in e} t_s = 1$.
Példa: Ha $\mathcal{V}(H) = \{1, 2, 3, 4\}$ és $\mathcal{E}(H) = \{\{1, 2\}, \{1, 4\}, \{3\}, \emptyset\}$ a $2; 1, 3; 0, 2; 1$ súlyokkal, akkor

$$Y_H = 2t_1t_2 + 1, 3t_1t_4 + 0, 2t_3 + 1.$$

Csonkított részhipergráfok: Tetszőleges (nemüres) A részhalmazára $\mathcal{V}(H)$-nak definiáljuk H_A-t (H A-csonkított részhipergráfját) a következőképpen:
$\mathcal{V}(H_A) = \mathcal{V}(H) \setminus A$
$\mathcal{E}(H_A) = \{B \subset \mathcal{V}(H_A) : B \cup A \in \mathcal{E}(H)\}$

Ha $B \in \mathcal{E}(H_A)$, akkor $w(B) = w(B \cup A)$.
Formálisan:

$$Y_{H_A} = \sum_{e:A\subset e} w(e) \prod_{i\in e\setminus A} t_i$$

Példa: A fentebbi H esetén legyen $A = \{1\}$, ekkor $Y_{H_A} = 2t_2 + 1, 3t_4$.
Az intuíciónk azt sugallja, hogy amennyiben egy Y pozitív polinom valamennyi (bármilyen rendű) parciális deriváltjának várható értéke szignifikánsan kisebb, mint Y-é, akkor Y erősen koncentrált. Ez magyarázza a csonkított részhipergráfok bevezetését, ugyanis az adott körülmények között Y_H parciális deriváltja $\{t_i : i \in A\}$ szerint éppen Y_{H_A}. Fontos azonban kiemelni, hogy csak az elsőrendű parciális deriváltak vizsgálata nem elégséges! Tekintsük ugyanis a következő példát: legyen m egy 4-gyel osztható pozitív egész szám és $l = m/4$. Legyenek $t_1, \ldots, t_m$ független azonos eloszlású valószínűségi változók $m^{-1/2}$ várható értékkel. Tekintsük a következő polinomot:

$$Y = \left(\sum_{i=1}^{l} t_{2i-1}t_{2i}\right)\left(\sum_{j=2l+1}^{m} t_j\right).$$

Könnyen kiszámolható, hogy Y várható értéke $\frac{m^{1/2}}{8}$, és Y bármely elsőrendű parciális deriváltjának várható értéke legfeljebb $1/2$. Másrészt viszont Y egyáltalán nem koncentrált! A Chernoff-egyenlőtlenség alkalmazásával belátható, hogy $1-o(1)$ valószínűséggel $\sum_{j=2l+1}^{m} t_j$ értéke legalább $\frac{m^{1/2}}{4}$, továbbá $\sum_{i=1}^{l} t_{2i-1}t_{2i}$ vagy 0, vagy legalább 1. Így Y értéke majdnem mindig 0 vagy legalább kétszerese a várható értékének! Ez a példa is azt igazolja, hogy az átlagos simaság definiálásához valamennyi parciális deriváltra szükség van. Térjünk tehát vissza további jelölések bevezetéséhez.

Jelölje $E_i(Y) = \max_{A\subset\mathcal{V}(H):|A|=i} E(Y_{H_A})$ – ekkor definíció szerint $E_0(Y)$ az Y várható értéke. Intuitív módon $E_i(Y)$ úgy tekinthető, mint i véletlen változó várható hatása. Legyen még $E = \max_{i\geq 0} E_i(Y)$ és $E' = \max_{i\geq 1} E_i(Y)$.

4.4. Lemma *Léteznek olyan csak k-tól függő c_k, d_k pozitív számok, hogy tetszőleges pozitív λ-ra*

$$P\left(|Y - E(Y)| \geq c_k(EE')^{1/2}\lambda^k\right) \leq d_k \exp(-\lambda + k\log n).$$

Szakdolgozatom során a 4.4-es lemmát csak $k \leq 5$ esetén fogjuk használni, ekkor igaz a következő is:

4.5. Következmény *Tegyük fel, hogy $k \leq 5$. A 4.4-es lemma feltételei mellett*

$$P\left(|Y - E(Y)| \geq (EE')^{1/2}\log^{k+1} n\right) = \exp(-\omega(\log n)),$$

azaz ha $n \to \infty$,

$$-\frac{\log P\left(|Y - E(Y)| \geq (EE')^{1/2}\log^{k+1} n\right)}{\log n} \to \infty.$$

A lemma következménye az is, hogy ha $E_0(Y)$ sokkal nagyobb, mint $\max_{i\geq 1} E_i(Y)$, akkor Y nagyon erősen koncentrálódik a várható értéke körül. Vegyük például azt az esetet, mikor k konstans, $n \to \infty$ és $E_0(Y) = E \geq E' \log^{2k+1} n$. Ekkor választhatjuk λ-t $\lambda = \log^{1+1/(3k)} n = \omega(\log n)$-nek, így a farok értéke $c_k(EE')^{1/2}\lambda^k = o(E) = o(E(Y))$ és a korlát $d_k \exp(-\lambda + k \log n) = \exp(-\omega(\log n))$.

A 4.4-es lemma erőssége abban áll, hogy csak a várható $E_i(Y)$ hatásokkal kell foglalkoznunk a legrosszabb eset hatása helyett, ami általában sokkal nagyobb. Azaz ha valószínűségi változók bármely, legfeljebb k elemű csoportjának átlagos hatása jelentősen kisebb, mint Y várható értéke, akkor Y erősen koncentrált. Így a fenti lemma számos olyan alkalommal is használható, ahol a klasszikus eszközök, mint például az Azuma-egyenlőtlenség, csődöt mondanak. A 4.5-ös következményből továbbá nyilvánvaló, hogy ha $k \leq 5$ és minden $i \geq 0$-ra az E_i értékek valamely konstanssal felülről becsülhetők, akkor igen nagy valószínűséggel Y $O(\log^{k+1} n)$-es.

A 4.4-es lemmát a következő módon fogjuk használni: ha adott egy Y függvény, először egy alacsonyfokú Y' polinommal közelítjük, majd az eredményeinket alkalmazva belátjuk, hogy Y' erősen koncentrált. Ha a közelítés elég jó, ebből már következni fog, hogy Y is erősen koncentrált. Ezt a közelítést kétféleképpen tehetjük meg: vagy megmutatjuk, hogy Y nagy valószínűséggel felülről (alulról) korlátos, és ekkor elég olyan Y' polinomot találni, ami felülről (alulról) korlátozza Y-t, és várható értékeik nagyjából egyenlők; vagy eleve olyan Y'-vel közelítünk, melynek várható értéke megegyezik Y-éval, erősen koncentrált és kis valószínűségű rossz esetek kivételével $Y = Y'$ – ahogy erről az előző szakaszban szó volt. A koncentrációs eredmény kidolgozása során főleg ez utóbbi módszer kapott nagy szerepet, azonban a szakdolgozatomban szereplő becslésekhez elegendő lesz az első típusú felső közelítés alkalmazása is (lásd később az 5. fejezet során), melyet *polinommódszer*nek nevezünk. Mielőtt azonban rátérnénk a konkrét részletekre, ahogy korábban megígértem, egy példán fogom demonstrálni a fentebbi koncentrációs eredmény erejét.

Példa: A $G(N,p)$ véletlen gráffal a fejezet bevezetőjében már találkoztunk, ahol felírtuk a gráfban szereplő háromszögek számára vonatkozó 4.1-es koncentrációs egyenlőtlenséget. Beláttuk, hogy az Azuma-egyenlőtlenség nem ad megoldást a problémánkra, ezért megpróbáljuk a fentebb ismertetett eredményeket – egészen pontosan a 4.4-es lemmát – alkalmazni. Ehhez vegyük észre, hogy Y (a háromszögek száma) felírható a következő harmadfokú polinomként:

$$Y = \sum_{1\leq i<j<l\leq N} t_{ij}t_{jl}t_{il},$$

ahol t_{ij} az ij élre vonatkozó választásunkat reprezentáló kétértékű véletlen változó. Nyilvánvaló, hogy t_{ij} és t_{ji} ugyanazt a változót jelölik.

Tudjuk, hogy $p = \Theta(N^{-3/4})$-re Y várható értéke $\Theta(N^3p^3) = \Theta(N^{3/4})$. Tegyük fel, hogy

$A = \{ij\}$, ekkor

$$Y_A = \sum_{l \neq i,j} t_{jl} t_{il}.$$

Könnyen látható, hogy

$$E(Y_A) = O(Np^2) = o(1).$$

Abban az esetben, ha A két elemből áll, akkor Y_A vagy 0, vagy t_{ij} valamely i-re és j-re. Végül pedig ha A-nak három eleme van, akkor Y_A vagy 0, vagy 1. Ebből következik, hogy

$$E'(Y) = \max_{i \geq 1} E_i(Y) = 1$$

és

$$E = \max_{i \geq 0} E_i(Y) = E(Y).$$

Legyen $\lambda = cN^{1/8}$, ahol a c pozitív konstansot úgy választjuk, hogy $c_3 \lambda^3 \sqrt{E(Y)} = \epsilon E(Y)$ legyen. Ekkor a 4.4-es lemma alapján

$$P(|Y - E(Y)| \geq \epsilon E(Y)) \leq d_3 e^{-\lambda + 3 \log n} = e^{-\Theta(N^{1/8})}.$$

Emlékezzünk vissza, hogy mind az Azuma-, mind a Talagrand-egyenlőtlenség csupán triviális felső becslést tudott adni a fenti valószínűségre, az új koncentrációs eredmény segítségével azonban megkaptuk a kívánt exponenciális korlátot.

4.4. A hatások korlátozása

A következőkben egy általános i lépést képzelünk el, ahol az input elemei Ω_i, S_i és A_i. Legyen $n = |S_i|$ és indexeljük S_i pontjait 1-től n-ig. Ebben a lépésben két forrása van a véletlennek: az egyik a *kiválasztás* művelet, a másik a *kompenzáció*. Éppen ezért jelölje t_j annak az eseménynek indikátorát, hogy a j-edik pontot kiválasztjuk a kiválasztás művelete során, u_j pedig legyen annak indikátora, hogy j-t töröljük a kompenzáció során. Együttesen tehát $2n$ független, kétértékű valószínűségi változónk van: a t_j-k független, azonos eloszlásúak; az u_j-k függetlenek, de nem feltétlenül azonos eloszlásúak (ahogy az a 2.2-es szakasz végén levő megjegyzésben szerepel). Rendezzük sorba a változóinkat (csupán a kényelmes jelölés miatt): $t_1, \ldots, t_n, t_{n+1} = u_1, \ldots, t_{2n} = u_n$.

Egy $L \subset S_i$, $|L| \geq \log^{100} q$ halmazra jelölje L' az i-edik lépés utáni túlélő pontjainak halmazát, azaz $L' = L \cap S_{i+1}$. Általában a következőt akarjuk majd megmutatni:

$$P(||L'| - E(|L'|)| \geq T) \leq \exp(-\omega(\log q)),$$

valamely alkalmas T hibataggal. Ahogyan korábban már szó volt róla, a t_j-knek igen nagy hatása lehet L'-re. Másrészt u_j hatása legfeljebb 1 lehet, és nincs hatása, ha $j \notin L$. Így

$\mathbb{B}_0(\mathbf{C},\mathbf{V})$-ben, a szórásnégyzet korlátok összegében (lásd a 4.2-as definíciót) az u_j-k hatása legfeljebb $|L|$-nyi hozzájárulást jelent. A következőkben olyan $\mathbf{C} \geq 1, \mathbf{V} \geq 2|L|$ értékeket vizsgálunk, amire

$$\mathbb{B}_0(\mathbf{C},\mathbf{V}) \subseteq \mathbb{B} := \mathbb{B}(\mathbf{C},\mathbf{V}) := \left\{ v \mid \max_{j=1,\dots,n} C_j(v) \geq \mathbf{C} \text{ vagy } \sum_{j=1}^{n} E(t_j)C_j(v) \geq \mathbf{V}/(2\mathbf{C}) \right\}. \tag{4.3}$$

Ezután már csak meg kell találnunk a $\mathbf{C}$ és $\mathbf{V}$ paramétereinket úgy, hogy

$$P(\mathbb{B}) = \exp(-\omega(\log q))$$

legyen (emlékeztetőül: a módszerünk egy kulcslépése a kis valószínűségű rossz eset kizárása – itt éppen azt fogalmazzuk meg, hogy a rossz eset valószínűsége kellően kicsi legyen).

Szakdolgozatom során mindvégig azt mondjuk majd, hogy egy A esemény *nagyon nagy valószínűséggel* bekövetkezik, ha $P(\overline{A}) = \exp(-\omega(\log q))$ – azaz a fentebbi feltétel éppen azt fogja jelenteni, hogy nagyon nagy valószínűséggel koncentrálódik a polinomunk. Mivel ebben a szakaszban egy általános, rögzített i lépésről beszélünk, a továbbiakban nem jelöljük az indexet, azaz A, S és p A_i, S_i és p_i helyett szerepel majd. Feltesszük még, hogy az algoritmus az $i-1$-edik lépésig tökéletesen fut. Tetszőleges j pontra legyen

$$A(L,j) = \{t \in L \mid (tj) \cap A \neq \emptyset\}$$

és $a(L) = \max\left\{\max_{j\in\Omega} |A(L,j)|, |L|\log^{-100} q\right\}$. Az imént bevezetett $a(L)$ mennyiség a következők miatt fontos: tegyük fel, hogy t_j értékét 1-ről 0-ra állítjva j kikerül az ívből. Ekkor mindazon $g \in L$ pontok, melyeket egy j-n és az aktuális A ív egy pontján átmenő szelő fedett, esélyt kapnak a túlélésre. Az ilyen pontok száma legfeljebb $a(L)$.

Sajnos azonban technikailag a dolog nem ennyire egyszerű, a fentebb említett szituáció mellett számos egyéb lehetőség is van – ezeket, mint nemsokára látni fogjuk, egy $\log q$-s faktor hozzáadásával aránylag könnyen kezelhetjük.

4.6. Lemma *A $C_k(v)$ hatás nagyon nagy valószínűséggel $o(\log q)a(L)$ nagyságrendű minden k-ra.*

4.7. Lemma *Nagyon nagy valószínűséggel*

$$\sum_{k=1}^{n} pC_k(v) = o(\log q)|L|.$$

A fenti két lemma gyakorlati következménye, hogy $\mathbf{C}$-t $a(L)\log q \geq 1$-nek és $\mathbf{V}$-t $a(L)|L|\log^4 q \gg |L|$-nek választhatjuk (lásd a 4.9-es lemmát).

A 4.6-os lemma bizonyítása: Tegyük fel, hogy t_k-t 1-ről 0-ra állítjuk. Jelölje H_k az átállítás hatását $|L'|$-re, ahol $t_1, t_2, \dots, t_{k-1}$ rögzített. Triviális felső becsléssel $H_k \leq \alpha + \beta$,

ahol α azon új pontok számát jelöli, melyek L'-be kerülnek, β pedig az átállítás miatt L-ből újonnan törlődő pontok száma. Fontos észben tartanunk, hogy C_k $t_1, \ldots, t_{k-1}$-től függő valószínűségi változó.
Jelölje $\sigma(k)$ a $t_1, \ldots, t_k$ által generált szigma-algebrát. Ekkor

$$C_k = |E\left(H_k|\sigma(k-1)\right)|\,. \tag{4.4}$$

Másrészt

$$H_k \leq \sum_{g \in L} H_k(g), \tag{4.5}$$

ahol $H_k(g) = 1$, ha t_k-t átállítva a g és L' közti tartalmazási reláció megváltozott, és 0 különben. Vegyük észre, hogy az egyetlen ok, amiért L' megváltozhat, az, hogy az új A' ív (emlékeztetőül: A jelöli A_i-t, A' pedig A_{i+1}-et) változott t_k átállításával. Az átállítás hatására A' egyetlen pontot veszthet, magát k-t, egyébként csak növelheti a méretét pár új ponttal (esetleg 0-val). Vizsgáljuk most ezen esetek hatását L'-re:

(a) Ha az A' ívhez új pontok adódnak, ezáltal L'-ből több pont kitörlődhet. Tegyük fel, hogy $g \in L$ egy ilyen pont, azaz g nem törlődött, mikor $t_k = 1$ volt, de törlődik, ahogy t_k értékét 0-ra állítjuk. Ehhez a következő esetek egyikének kell bekövetkeznie:

(I) Vannak olyan j és $a, b \in A$ pontok, hogy $t_j = 1, [gaj]$ és $[jkb]$. Ekkor a következő történhet: t_k-t átállítva j bekerülhet A'-be és ezzel g törlődik, mivel g, j és a egy egyenesen vannak.

(II) Létezik olyan $a \in A$ és j, j', hogy $t_j = t_{j'} = 1$ és $[ajg], [jj'k]$. Ebben az esetben k törlésével mind a j, mind a j' bekerülhet, ezáltal g törlődik.

(III) Van olyan j, j', hogy $t_j = t_{j'} = 1, [gjj']$ és a (jk) egyenes metszi A-t. Ekkor ha t_k-t 0-ra állítjuk, j hozzáadódhat A-hoz, ami $[gjj']$ miatt g törléséhez vezethet.

(IV) Léteznek olyan j, j', j'' pontok, hogy $t_j = t_{j'} = t_{j''} = 1$ és $[gjj'], [jj''k]$ teljesül. Ilyenkor k törlésével j (és j'') bekerülhet A-ba, ami $[gjj']$ miatt g törlését okozhatja.

(b) Ha t_k átállításával az új A' ív pontot veszít, az csak akkor történhet meg, ha a k pont az átállítás előtt A'-ben volt. Ebben az esetben L' új pontokat nyerhet. Ha g ilyen pont, azaz g törlődött, amikor $t_k = 1$ volt, és túlél, ha $t_k = 0$, az csak a következő szituációk valamelyikének fennállása esetén történhet:

(V) Van olyan $a \in A$ pont, hogy $[gak]$ teljesül. Ilyenkor ugyanis az ív definíciója szerint g nem kerülhet bele A-ba, mert ütközést okozna, emiatt törlődne L-ből. Ha viszont k-t töröljük, akkor g esélyt nyer a következő fordulóra, és bekerülhet L'-be.

(VI) Létezik olyan j, hogy $t_j = 1$ és $[gjk]$ igaz. Ebben az esetben g az algoritmus leírása alapján törlődne L-ből, de ha k kikerül A'-ből, akkor g (és j is) esélyt kap a túlélésre.

A következő lépésben $\sum_g H_k(g)$-t a fenti hat esetnek megfelelően hat tagra ($H_k(I)$-től $H_k(VI)$-ig) bontjuk szét. Mivel csak H_k felső becslésére van szükségünk, az esetek közti átfedésektől eltekinthetünk. Először becsüljük $H_k(I)$-t. Vegyük észre, hogy (az (I)-es eset érvelésének megfelelően)

$$H_k(I) \leq \sum_{j \neq k} t_j \mathbf{1}_{\{j \in A(k)\}} \sum_{g \in L} \mathbf{1}_{\{j \in A(g)\}} \leq \sum_{j \in A(k)} t_j |A(L,j)|.$$

C_k-t hasonlóan hat részre szétbontva, és felhasználva, hogy $j < k$ esetén t_j mérhető $\sigma(k-1)$-re, ha pedig $j > k$, akkor független tőle:

$$C_k(I) = E\left(H_k(I)|\sigma(k-1)\right) \leq \sum_{j \in A(k), j<k} t_j |A(L,j)| + \sum_{j \in A(k), j>k} p|A(L,j)|. \tag{4.6}$$

A jobboldal második tagja $O(1)$-es, mivel

$$\sum_{j \in A(k), j>k} p|A(L,j)| \leq a(L)p|A(k)|,$$

ahol $A(k) = A_i(k)$ definícióját lásd a 2.3-as fejezetben. Mivel feltettük, hogy az algoritmus az aktuális állapotig tökéletesen fut, ezért (a **(12)**-es tulajdonság alapján) $|A(k)| \sim a_i b_i q^{3/2}$, $p = p_i$ pedig $\theta(b_i q^{3/2})^{-1}$. Így

$$a(L)p|A(k)| \leq 2a_i \theta a(L) \sim i\theta^2 a(L) \leq \log^{-1} q\, a(L) = o(a(L)).$$

Tekintsük most a 4.6-os jobboldalának első tagját, ami független véletlen változók összege. Mivel $\sum_{j \in A(k), j<k} t_j$ várható értéke legfeljebb $a_i\theta = o(1)$, nagyon nagy valószínűséggel az összeg $o(\log q)$-s. Összességében tehát nagyon nagy valószínűséggel

$$C_k(I) = o(\log q)a(L). \tag{4.7}$$

A (II-IV) esetek hasonlóan kezelhetők, a részleteket elhagyjuk. Az (V)-ös pont esetében ($A(L,j)$ definíciójából) világos, hogy a szóba jöhető g pontok száma legfeljebb $\max_j |A(L,j)| \leq a(L)$. Végül a bizonyítás teljessé tételéhez vizsgáljuk a (VI)-os szituációt. Az (I)-esnél látotthoz hasonló érveléssel kapjuk, hogy

$$H_k(VI) \leq \sum_{t \in L} \sum_{j:[jkt]} t_j.$$

Ebből

$$C_k(VI) \leq \sum_{t \in L} \sum_{j:[jkt], j<k} t_j + \sum_{t \in L} \sum_{j:[jkt], j>k} p = Z.$$

Először tegyük fel, hogy az algoritmus első fázisában vagyunk. A jobboldal első tagjának várható értéke – mivel feltettük, hogy az algoritmus az aktuális állapotig tökéletesen fut, ezért minden j-re vagy k-ra illeszkedő egyenesnek kevesebb, mint $2b_iq$ túlélő pontja van – legfeljebb (feltéve, hogy q megfelelően nagy) $|L|2b_iqp_i \leq |L|q^{-1/2} \leq |L|\log^{-102} q$. A második tag várható értéke ugyanígy adódik, így összességében $E(Z) \leq 2|L|\log^{-102} q$. Független tagú összegekről lévén szó könnyen megmutatható (például a 4.4-es lemma segítségével), hogy nagyon nagy valószínűséggel $Z \leq |L|\log^{-100} q \leq a(L)$.

Utolsó lépésként tegyük fel, hogy a második fázisban vagyunk. Ekkor használjuk ki azt a tulajdonságot, hogy minden egyenesnek legfeljebb $2\log^{c_1} q$ pontja van (ez az első fázis második tulajdonságának és a második fázis definíciójának következménye). Ha ezt tudjuk, $E(Z) \leq 2 \cdot 2|L|p_i \log^{c_1} q$. Másrészt itt $p_i = \theta(b_iq^{3/2})^{-1} \leq \log^{-c} q$ az algoritmus leírása alapján. Ezért $E(Z) \leq |L|\log^{c_1-c} q \leq |L|\log^{-101,5} q$ (emlékeztetőül: $c = 300$ és $c_1 = 100$). A 4.4-es lemma ismételt alkalmazásával kaphatjuk, hogy nagyon nagy valószínűséggel $Z \leq |L|\log^{-100} q \leq a(L)$. ■

A 4.7-es lemma bizonyítása: Ismét bontsuk fel C_k-t hat tag $(C_k(I) - C_k(VI))$ összegére. Tekintsük az elsőt:

$$p\sum_{k=1}^{n} C_k(I) \leq p\sum_{k=1}^{n}\left(\sum_{j\in A(k),j<k} t_j|A(L,j)| + \sum_{j\in A(k),j>k} p|A(L,j)|\right).$$

Vágjuk szét a jobboldalt egy konstans és független véletlen változók összegére.
A konstans a következő:

$$p\sum_{k=1}^{n}\sum_{j\in A(k),j>k} p|A(L,j)| \leq p^2\sum_{j=1}^{n}|A(L,j)||\{k \ : \ j \in A(k)\}| =$$

$$= p^2\sum_{j=1}^{n}|A(L,j)||A(j)| \leq p^2\max_j|A(j)|\sum_{j=1}^{n}|A(L,j)| =$$

$$= p^2\max_j|A(j)|\sum_{t\in L}|A(t)| \leq |L|p^2(\max_j|A(j)|)^2.$$

Emlékeztetőül, az i-edik lépésben $p\max_j|A(j)| \sim a_i\theta = o(1)$. Így az utolsó formula $o(|L|)$-es.
Következő lépésként megmutatjuk, hogy a másik tag, ami véletlen változók összege, nagyon nagy valószínűséggel $o(\log q)|L|$ nagyságrenddel felülről korlátos. A kérdéses összeg

$$p\sum_{k=1}^{n}\sum_{j\in A(k),j<k} t_j|A(L,j)|, \tag{4.8}$$

ami felülről becsülhető a következő mennyiséggel:

$$p\max_j|A(j)|\sum_{j=1}^{n} t_j|A(L,j)|.$$

A $\sum_{j=1}^{n} t_j|A(L,j)|$ kifejezés várható értéke $p\sum_{j=1}^{n}|A(L,j)| = p\sum_{j\in L}|A(j)|$. Ahogy korábban már megmutattuk, ez utóbbi mennyiség legfeljebb $p|L|\max_{t\in L}|A(t)| = o(|L|)$. Ennek ismeretében már könnyű belátni, hogy nagyon nagy valószínűséggel $\sum_{j=1}^{n} t_j|A(L,j)|$ $O(\log q)$ nagyságrendű, mivel $|A(L,j)| \le |L|$. Ezért a 4.8-as (nagyon nagy valószínűséggel) legfeljebb $p\max_j|A(j)|O(\log q)|L| = o(\log q)|L|$, mivel $p\max_j|A(j)| = o(1)$. A hátralevő (II-VI) esetek bizonyítása teljesen hasonló elven működik. ■

4.8. Megjegyzés Ebben és az előző szakaszban az egyszerűség kedvéért feltettük, hogy $L \subset S$. Azonban minden állításunk $L \subset \Omega$ esetén is teljesül: az előző szakasz vizsgálatánál az $L \setminus S$-be eső pontok csak segíthetnek, mivel a kompenzáció művelet rájuk nem hat; a fenti szakaszban pedig sehol nem használtuk ki, hogy $L \subset S$.

4.5. Következtetések

4.9. Lemma *Rögzítsünk egy L halmazt Ω-ban. Ekkor nagyon nagy valószínűséggel*

$$|L' - E(L')| \le a(L)^{1/2}|L|^{1/2}\log^5 q.$$

Bizonyítás: Legyen $\mathbf{C} = a(L)\log q, \mathbf{V} = a(L)|L|\log^4 q$ és $\lambda = \log^{3/2} q$. A 4.3-as lemma alapján

$$P\left(|L' - E(L')| \ge (\lambda\mathbf{V})^{1/2}\right) \le \exp(-\omega(\log q)) + P(\mathbb{B}),$$

ahol $\mathbb{B}$ definícióját lásd a 4.2-es fejezetben. Könnyen kapható, hogy (tág becsléssel) $(\lambda\mathbf{V})^{1/2} = o(a(L)^{1/2}|L|^{1/2}\log^5 q)$. Másrészt a 4.6-os és 4.7-es lemmák alapján

$$P(\mathbb{B}) = \exp(-\omega(\log q)),$$

ami teljessé teszi a bizonyítást. ■

A lemmának azonnali következménye:

4.10. Következmény *Legyen K rögzített pozitív konstans. Ekkor tetszőleges L halmazra, melyre $a(L) \le \frac{|L|}{\log^{2(K+5)} q}$, nagyon nagy valószínűséggel $|L' - E(L')| \le |L|\log^{-K} q$ teljesül.*

A fő lemma bizonyítása során gyakran lesz szükségünk a következő formájú állítások igazolására: „igen nagy valószínűséggel $|L - E(L)| \le |L|\log^{-d} q$", ahol d alkalmasan választott konstans (megfigyelhető, hogy a fő lemma tulajdonságaiban szereplő valamennyi hibatag $\log^{-d} q$ alakú valamely d-re).
Vizsgálva az $a(L) = \max\left\{\max_{j\in\Omega}|A(L,j)|, |L|\log^{-100} q\right\}$ mennyiséget nyilvánvaló, hogy ha $a(L) = |L|\log^{-100} q$, akkor a 4.9-es lemma vagy a 4.10-es következmény azonnal igazolná a fenti típusú állítást (d értéke valamennyi alkalmazás során sokkal kisebb lesz, mint 100, így a kitevőben szereplő 100-as konstans tág teret nyújt majd). Emiatt viszont csak az $a(L) = \max_{j\in\Omega_i}|A(L,j)|$ esetre kell koncentrálnunk, és ennek fennállását a 4.9-es lemma vagy a 4.10-es következmény minden alkalmazása során fel is tesszük.

5. fejezet

A fő lemma bizonyítása

A bizonyítás során ismét egy általános i lépéssel dolgozunk, mindvégig feltéve, hogy az algoritmus az $i-1$-edik lépésig tökéletesen fut – ez a feltétel az indukciós hipotézisünk ($i=1$-re a tulajdonságok triviálisan teljesülnek). Az indukciós bizonyítás elve alapján azt kell tehát megmutatnunk, hogy valamennyi tulajdonság nagyon nagy valószínűséggel teljesül i-re is. Mivel a tulajdonságok száma (figyelembe véve az összes lehetséges választást l, u, v, w, z-re) $O(q^{10})$, az is következik majd, hogy nagyon nagy valószínűséggel a tulajdonságok együttesen is fennállnak.

5.1. Első fázis

Az első fázis tíz tulajdonságát négy csoportba soroljuk: **(1)**; **(2)(4)(5)**; **(3)(9)(10)** és **(6)(7)(8)**. Az utolsó három csoport esetében alkalmazott stratégia hasonló: először mindnél bebizonyítjuk a legmagasabb indexű tulajdonságot (**(5), (10), (8)**), a 4.3-as fejezet végén bemutatott polinommódszert alkalmazva. Következő lépésként a középső tulajdonságokat (**(4), (9), (7)**) igazoljuk a 4.9-es lemma és ismét a polinommódszer felhasználásával. Azért kell először a magasabb indexű tulajdonságokat igazolnunk, mert az ezekben megjelenő mennyiségek játsszák $a(L)$ szerepét (lásd a 4.9-es lemmában) a **(4), (9), (7)**-es tulajdonságokban megjelenő mennyiségekre nézve. Teljesen hasonlóan, a **(4), (9), (7)**-es tulajdonságokban szereplő mennyiségek adják $a(L)$-t a **(2), (3), (6)**-os tulajdonságok mennyiségeire nézve. Így a 4.9-es lemma újbóli alkalmazásával bizonyíthatjuk ez utóbbiakat. Az **(1)**-es tulajdonság igazolása teljes egészében a polinommódszerre épül. A **(6)**-os tulajdonság, bár nem elsődleges, kiemelt fontosságú szerepet játszik a második fázis elemzésében, erre később még visszatérünk.

5.1.1. (1)-es

$$\theta q^{1/2}(1-o(1)) \leq |M_i| \leq \theta q^{1/2}(1+o(1))\mathrm{s}|B_i| \leq 2\theta q^{1/2}$$

Legyen $U_i = B_i \setminus M_i$. Az állítás igazolásához elég megmutatni, hogy nagyon nagy valószínűséggel $|B_i| \leq (1+o(1))\theta q^{1/2}$ és $|U_i| = o(1)\theta q^{1/2}$. Az első egyenlőtlenség könnyen belátható például a 4.4-es lemma alkalmazásával, felhasználva, hogy B_i független azonos eloszlású véletlen változók összege és $E(B_i) = \theta q^{1/2} \geq \log^2 q$. A második igazolásához a 4.3-as fejezet utolsó szakaszában bemutatott polinommódszert fogjuk alkalmazni. Ehhez $|U_i|$-t először egy alacsonyfokú polinommal becsüljük a következőképpen: vegyük észre, hogy tetszőleges $j \in U_i$ pontra j kiválasztott (azaz $t_j = 1$), de nincs benne M_i-ben. Ez utóbbinak két lehetséges oka van: az első, hogy van olyan $j' \in B_i$ pont, hogy (jj') metszi A_i-t, azaz $\sum_{j' \in A_i(j)} t_{j'} \geq 0$. A második, hogy van két olyan j', j'' pont B_i-ben, hogy j, j' és j'' egy egyenesre esik. Ez akkor lehetséges, ha $\sum_{j',j'':[jj'j'']} t_{j'}t_{j''} \geq 0$. Összességében tehát

$$|U_i| = \sum_{j \in S_i} t_j \mathbf{1}_{j \notin M_i} \leq \sum_{j \in S_i} t_j \left(\sum_{j' \in A_i(j)} t_{j'} + \sum_{j',j'':[jj'j'']} t_{j'}t_{j''} \right). \tag{5.1}$$

Tekintsük a jobboldal első összegét:

$$\sum_{j \in S_i} t_j \sum_{j' \in A_i(j)} t_{j'} = \sum_{j \in S_i, j' \in A_i(j)} t_j t_{j'} = Y.$$

Y becsléséhez a 4.4-es lemmát alkalmazhatjuk, mivel Y egy másodfokú polinom. Továbbá az indukciós hipotézis miatt $|S_i| = b_i q^2, a_i \sim i\theta$ és $|A_i(j)| \sim a_i q^{1/2}(b_i q) \leq 2a_i b_i q^{3/2}$. Így

$$E_0(Y) = E(Y) \leq 2(b_i q^2)(a_i b_i q^{3/2}) p_i^2 = 2a_i \theta^2 q^{1/2}.$$

$E_1(Y)$ becsléséhez figyeljük meg, hogy tetszőleges rögzített j esetén legfeljebb $\max_j |A_i(j)|$ olyan j' pont van, hogy a $t_j t_{j'}$ szorzat szerepel Y-ban (emlékeztetőül, $E_1(Y)$ nem más, mint azon várható értékek maximuma, melyeket úgy kapunk, hogy Y-ból egy változót lerögzítünk, és csak azokat az „éleket" vesszük figyelembe (változatlan súllyal), melyekben a rögzített változó szerepel), és ahogy fentebb említettük, $|A_i(j)| \leq 2a_i b_i q^{3/2}$. Így

$$E_1(Y) \leq 2(a_i b_i q^{3/2}) p_i = 2a_i \theta \leq 4i\theta^2 = o(1),$$

ahol az utolsó egyenlőtlenség során felhasználtuk azt a tényt, hogy $i = O(\theta^{-1} \log^{1/2} q)$ (lásd az algoritmus futásidejéről szóló 3.5-ös lemmát) és $\theta = \log^{-2} q$.
Végül vegyük észre, hogy bármely $t_j t_{j'}$ szorzat legfeljebb kétszer jelenhet meg, ezért $E_2(Y) \leq 2$. Így a 4.4-es lemma alapján nagyon nagy valószínűséggel

$$Y \leq 3a_i \theta^2 q^{1/2} = o(\theta q^{1/2}).$$

Hasonló érveléssel ugyanezt igazolhatjuk az 5.1-es másik tagjára is, azaz hogy nagyon nagy valószínűséggel

$$\sum_{j \in S_i} t_j \left(\sum_{j',j'':[jj'j'']} t_{j'}t_{j''} \right) = o(\theta q^{1/2}),$$

ami teljessé teszi a bizonyítást. ■

5.1. Megjegyzés Részletesebb számításokkal megmutatható, hogy a második tag (nagyon nagy valószínűséggel) $10\theta^3 q^{1/2}$-nel is becsülhető. Ennek alapján

$$a_{i+1} - a_i \geq \theta - (3a_i\theta^2 + 10\theta^3).$$

Továbbá az is igazolható, hogy nagyon nagy valószínűséggel $|B_i| \leq (\theta + \theta^3)q^{1/2}$. Így $a_{i+1} - a_i \leq \theta + \theta^3$.

5.1.2. (5)-ös

$$|S_{i+1}(l,u,v)| \leq (i+1)\log^4 q$$

Tekintsünk egy l egyenest és jelöljük $B_i(l,v)$-vel azon $x \in l$ pontok halmazát, melyekre a (vx) egyenes metszi B_i-t. Legyen továbbá $B_i(l,u,v) = B_i(l,u) \cap B_i(l,v)$. Vegyük észre, hogy tetszőleges $x \in S_{i+1}(l,u,v) \setminus S_i(l,u,v)$ pont a következők egyikébe kell tartozzon: $B_i(l,u,v); S_i(l,u) \cap B_i(l,v)$ vagy $S_i(l,v) \cap B_i(l,u)$. Ebből következik, hogy

$$|S_{i+1}(l,u,v)| \leq$$

$$\leq |S_i(l,u,v)| + |B_i(l,u,v)| + |S_i(l,u) \cap B_i(l,v)| + |S_i(l,v) \cap B_i(l,u)|.$$

Az indukciós hipotézis alapján $|S_i(l,u,v)| \leq i\log^4 q$, ezért elég megmutatni, hogy a jobboldalon szereplő utolsó három tag nagyon nagy valószínűséggel legfeljebb $\frac{1}{3}\log^4 q$.
Tekintsük először az elsőt, $|B_i(l,u,v)|$-t. Az **(1)**-es tulajdonság igazolásához hasonlóan ismét a polinommódszert fogjuk alkalmazni. Vegyük észre, hogy ha egy $x \in l$ pont $B_i(l,u,v)$-be esik, akkor léteznek olyan $j \in (xu)$ és $j' \in (xv)$ pontok, hogy j-t és j'-t is kiválasztottuk B_i-be (azaz $t_j = t_{j'} = 1$). Ezért

$$B_i(l,u,v) \leq \sum_{x \in l} \left(\sum_{j \in (xu)} t_j \right) \left(\sum_{j' \in (xv)} t_{j'} \right) = \sum_{jj' \in \mathcal{E}(H)} t_j t_{j'} = Y,$$

ahol H egy S_i-n értelmezett gráf, élhalmaza, $\mathcal{E}(H)$ mindazon jj' párokból áll, melyeket a két összeg szorzatából nyerünk.
A következő lépésben megmutatjuk, hogy nagyon nagy valószínűséggel $Y = O(\log^3 q) \ll \frac{1}{3}\log^4 q$. Ez a 4.4-es lemma azonnali következménye lesz, csupán azt kell még megmutatnunk, hogy $E_i(Y) = O(1)$ $i = 0,1,2$ esetén. Nyilvánvaló, hogy $E_2(Y) \leq 2$, mivel minden (j,j') pár legfeljebb kétszer szerepelhet. Továbbá

$$E_0(Y) \leq p_i^2 (\max_{l'} |S_i(l')|)^2 \leq 4p_i^2 (b_i q)^2 = 4\theta^2 q^{-1} \leq 1,$$

ahol kihasználtuk, hogy $|S_i(l')| \leq 2b_i q$ minden l' egyenesre (ahogy feltettük, hogy az algoritmus az $i-1$-edik lépésig tökéletesen fut), és $p_i = \theta(b_i q^{3/2})^{-1}$. Hasonlóan

$$E_1(Y) \leq p_i \max_{l'} |S_i(l')| \leq 2\theta q^{-1/2} \leq 1.$$

A másik két tag becslése ugyanezen az elven működik. ■

5.1.3. (4)-es

$$|S_{i+1}(l,v)| \le 8(i+1)a_{i+1}b_{i+1}q^{1/2} + (i+1)\log^{40} q$$

A 4.4-es és 4.5-ös fejezetek eredményeit alkalmazandó definiáljuk L-et $S_i(l,v)$-ként. Az indukciós hipotézis alapján $|S_i(l,v)| \le 8ia_ib_iq^{1/2} + i\log^{40} q$. Ahogy a 4.4-es szakaszban, legyen L' L túlélő pontjainak halmaza – világos, hogy tetszőleges $x \in S_{i+1}(l,v)\setminus L'$ pontnak $B_i(l,v)$-ben kell lennie. Ezért

$$|S_{i+1}(l,v)| \le |L'| + |B_i(l,v)|. \tag{5.2}$$

A jobboldal tagjait egyenként becsüljük. Először tekintsük L'-t:

$$E(|L'|) = |L|(1-P_i^u) \le 8ia_ib_{i+1}q^{1/2} + i\log^{40} q, \tag{5.3}$$

mivel definíció szerint $b_{i+1} = b_i(1-P_i^u)$. Vegyük észre, hogy az **(5)**-ös tulajdonság bizonyítása alapján ($a(L)$ esetünkben $S_i(l,u,v)$-nek felel meg)

$$a(L) \le \max_{l,u,v} |S_i(l,u,v)| \le i\log^4 q \le \log^7 q,$$

hiszen $i \le \log^3 q$. Ezért a 4.9-es lemma miatt nagyon nagy valószínűséggel

$$|L'| \le E(L') + E(L')^{1/2}\log^9 q. \tag{5.4}$$

(Itt kihasználtuk, hogy $P_i^u = o(1)$-es (lásd a 3.8-es megjegyzést), ezért $|L|$ helyett $E(L')$-t írhattunk a felső becslésben.)
Következő lépésként becsüljük a polinommódszer segítségével $B_i(l,v)$-t. Az algoritmus leírásából következik, hogy ha egy x pont $B_i(l,v)$-ben van, akkor az (xv) egyenes valamely j pontjának kiválasztottnak kell lennie, azaz $t_j = 1$. Ezért

$$|B_i(l,v)| \le \sum_{x\in l}\sum_{j\in(xv)} t_j = Y.$$

A 4.4-es lemma használatához becsüljük a várható értékeket: az indukciós hipotézis alapján $|S_i(l')| \sim b_iq \le 2b_iq$ tetszőleges l' egyenesre, így

$$E_0(Y) \le p_i \max_{l'} |S_i(l')|^2 \le p_i(2b_iq)^2 = 4\theta b_iq^{1/2}. \tag{5.5}$$

Továbbá, mivel bármely j pont legfeljebb egyszer jelenhet meg, $E_1(Y) = 1$. Ezért a 4.4-es lemma alapján nagyon nagy valószínűséggel

$$|B_i(l,v)| \le E(Y) + (\max(E(Y),1))^{1/2}\log^2 q. \tag{5.6}$$

Az 5.2–5.6-os egyenlőtlenségek alapján a következőt kapjuk (nagyon nagy valószínűséggel):

$$|S_{i+1}(l,v)| \le 8ia_ib_{i+1}q^{1/2} + i\log^{40} q + \left(ia_ib_{i+1}q^{1/2} + i\log^{40} q\right)^{1/2}\log^9 q +$$

$$+4\theta b_i q^{1/2} + \max(4\theta b_i q^{1/2}, 1)^{1/2} \log^2 q. \tag{5.7}$$

Emlékeztetőül, $a_i \sim i\theta, 1, 1b_i \geq b_{i+1} \geq 0, 9b_i$, $i \leq \log^3 q$ (ezek a becslések az indukciós hipotézis alapján működnek).Továbbá az **(1)**-esre alapozva $a_{i+1} \sim a_i + \theta$. Ezeket felhasználva belátjuk, hogy az 5.7-es jobboldala legfeljebb

$$8(i+1)a_{i+1}b_{i+1}q^{1/2} + (i+1)\log^{40} q,$$

igen tág becsléssel a logaritmus kitevőjében.
Ennek érdekében vegyük észre, hogy

$$8(i+1)a_{i+1}b_{i+1}q^{1/2} - 8ia_ib_{i+1}q^{1/2} \geq 8a_ib_{i+1}q^{1/2},$$

ezért csak azt kell megmutatnunk, hogy

$$8a_ib_{i+1}q^{1/2} + \log^{40} q \geq \tag{5.8}$$

$$\geq \left(ia_ib_{i+1}q^{1/2} + i\log^{40} q\right)^{1/2} \log^9 q + 4\theta b_i q^{1/2} + \max(4\theta b_i q^{1/2}, 1)^{1/2} \log^2 q.$$

Abban az esetben, ha $b_i q^{1/2} > \log^{36} q$, akkor

$$\max(4\theta b_i q^{1/2}, 1)^{1/2} \log^2 q \leq 3\theta b_i q^{1/2}$$

és

$$\left(ia_ib_{i+1}q^{1/2} + i\log^{40} q\right)^{1/2} \log^9 q \leq a_ib_{i+1}q^{1/2}.$$

Így az 5.8-as jobboldala legfeljebb

$$4\theta b_i q^{1/2} + 3\theta b_i q^{1/2} + a_ib_{i+1}q^{1/2} \leq 8a_ib_{i+1}q^{1/2}.$$

Végül tegyük fel, hogy $b_i q^{1/2} \leq \log^{36} q$. Ebben az esetben könnyű ellenőrizni, hogy az 5.8-as baloldalán szereplő $\log^{40} q$-s tag minden hibatagot dominál, és ez teljessé teszi a bizonyításunkat. ■

5.1.4. (2)-es

$$b_{i+1}q(1 - (i+1)\log^{-13} q) \leq |S_{i+1}(l)| \leq b_{i+1}q(1 + (i+1)\log^{-13} q)$$

Az előző két bizonyítás tulajdonképpen a **(2)**-es igazolását célozta: valójában csak erre a tulajdonságra van szükségünk a háromból, azonban a másik két tulajdonság nélkül a bizonyítás nem működik. Legyen tehát $L = S_i(l)$ és $K = 14$ (hogy a 4.10-es következményt alkalmazhassuk). Vegyük észre, hogy a **(4)**-es tulajdonság alapján

$$a(L) \leq \max_{l',v} |S_i(l', v)| = O(ia_ib_iq^{1/2} + i\log^{40} q).$$

Továbbá az indukciós hipotézis okán $|L| \sim b_i q \geq \frac{1}{2} b_i q$. Mivel az algoritmus első fázisában vagyunk, $b_i q \geq \log^{100} q$, így $b_i q \geq a(L) \log^{2(K+5)} q$. Ezért a 4.10-es következmény alapján nagyon nagy valószínűséggel

$$\big||L'| - E(|L'|)\big| \leq |L| \log^{-14} q \leq 2 b_i q \log^{-14} q,$$

ahol L' szokásosan $S_{i+1}(l)$-et jelöli.
Figyeljük meg, hogy ha $|L| = b_i q(1+\alpha)$, akkor $E(|L'|) = b_{i+1} q(1+\alpha)$. Ezért az indukció alapján $E(|L'|)$-re teljesül, hogy $|E(|L'|) - b_{i+1} q| \leq i b_{i+1} q \log^{-13} q$. Végül a háromszög-egyenlőtlenség alapján

$$\big||L'| - b_{i+1} q\big| \leq \big(i \log^{-13} q + 2 \log^{-14} q\big)\, b_{i+1} q \leq (i+1) b_{i+1} q \log^{-13} q,$$

kihasználva, hogy $b_{i+1} \sim b_i$. ■

5.1.5. (3)-as, (9)-es, (10)-es

$$\textbf{(3)} \quad |\Omega_{i+1}(l)| \leq b'_{i+1} q (1 + (i+1) \log^{-13} q)$$

$$\textbf{(9)} \quad |\Omega_{i+1}(l,v)| \leq 8(i+1) a_{i+1} b'_{i+1} q^{1/2} + (i+1) \log^{40} q$$

$$\textbf{(10)} \quad \Omega_{i+1}(l,u,v)| \leq (i+1) \log^4 q$$

Az ebben a csoportban szereplő tulajdonságok bizonyítása többé-kevésbé megegyezik az előző csoportéval; az egyetlen formális különbség, hogy b_i helyett b'_i-t használunk, valamint hogy a **(3)**-asban csak felső becslésre van szükségünk. ■

5.1.6. (8)-as

$$|A_{i+1}(u,v,w,z)| \leq (i+1) \log^6 q$$

Legyen $X = \{u,v,w,z\}$, és tetszőleges nemüres X' részhalmazára legyen $A_i(X') = \cap_{a \in X'} A_i(a)$ és $B_i(X') = \cap_{a \in X'} B_i(a)$. Első lépésként vegyük észre, hogy

$$A_{i+1}(X) \subset A_i(X) \cup B_i(X) \cup \sum_{X' : 1 \leq |X'| \leq 3} A_i(X') \cap B_i(X \setminus X').$$

(Emlékeztetőül: $A_i(v)$ a v-t A_i-beli pontokkal összekötő egyeneseken levő túlélő pontok halmaza (kivéve v-t magát).) Ezért elég csak annyit belátnunk, hogy nagyon nagy valószínűséggel $|B_i(X)| \leq \log^5 q$ és $|A_i(X') \cap B_i(X \setminus X')| \leq \log^5 q$ minden megfelelő X' részhalmazra. Az első becsléshez használjuk ki, hogy definíció szerint tetszőleges $x \in B_i(X)$-hez kell legyen olyan $j, j', j'', j''' \in B_i$, melyekre $[jxu], [j'xv], [j''xw]$ és $[j'''xz]$ teljesül. Emiatt

$$B_i(X) \leq \sum_{x \in S_i} \left(\sum_{j : [jxu]} t_j \right) \left(\sum_{j' : [j'xv]} t_{j'} \right) \left(\sum_{j'' : [j''xw]} t_{j''} \right) \left(\sum_{j''' : [j'''xz]} t_{j'''} \right) =$$

$$= \sum_{(j,j',j'',j''')\in\mathcal{I}} t_j t_{j'} t_{j''} t_{j'''} = Y,$$

ahol $\mathcal{I}$ az összes lehetséges (j, j', j'', j''') négyesből álló indexhalmaz.
Mivel Y egy negyedfokú polinom, a bizonyítás befejezéséhez használhatjuk a 4.5-ös következményt. Ehhez elég megmutatni, hogy $E_i(Y) = O(1)$ ha $0 \le i \le 4$. Nyilvánvalóan $E_4(Y) = 1$. Továbbá

$$E_0(Y) \le p_i^4 |S_i| (\max_l |S_i(l)|)^4 \le 2p_i^4 b_i q^2 (b_i q)^4 = 2\theta^4 b_i = O(1),$$

$$E_1(Y) \le p_i^3 (\max_l |S_i(l)|)^4 \le 2p_i^3 (b_i q)^4 = 2\theta^3 b_i q^{-1/2} = O(1),$$

$$E_2(Y) \le p_i^2 (\max_l |S_i(l)|)^2 \le 2p_i^2 (b_i q)^2 = 2\theta^2 q^{-1} = O(1),$$

$$E_3(Y) \le p_i (\max_l |S_i(l)|) \le 2p_i (b_i q) = 2\theta q^{-1/2} = O(1)$$

Az $|A_i(X') \cap B_i(X \setminus X')|$-re vonatkozó bizonyítás hasonlóan működik, ebben az esetben az eredményül kapott polinom foka $|X \setminus X'|$, így $\log^5 q$ helyett $\log^4 q$-s felső korláttal dolgozhatunk, ez azonban nem okoz lényegi különbséget. ■

5.1.7. (7)-es

$$|A_{i+1}(u, v, w)| \le (i + 1)b_{i+1} q^{1/2} + (i + 1) \log^{22} q$$

Legyen $X = \{u, v, w\}$, ahol u, v és w tetszőleges Ω_i-beli pontok. Definiáljuk L-et $A_i(u, v, w)$-nek és L'-t $L \cap S_{i+1}$-nek. Ahogyan az előző bizonyításban, úgy kapjuk most is:

$$|A_{i+1}(X)| \le |L'| + |B_i(X)| + \sum_{X' \subset X} |A_i(X') \cap B_i(X \setminus X')|, \tag{5.9}$$

ahol az utolsó összeget X összes alkalmas X' részhalmazára vesszük.
Mivel tetszőleges S_i-beli pont $1 - P_i^u$ valószínűséggel él túl, ezért

$$E(|L'|) \le \left(i b_i q^{1/2} + i \log^{22} q \right) (1 - P_i^u) \le i b_{i+1} q^{1/2} + i \log^{22} q.$$

Másrészt a **(8)**-as miatt

$$a(L) \le \max_{z\in\Omega_i} |A_i(u, v, w, z)| \le i \log^6 q \ll \log^9 q. \tag{5.10}$$

Így a 4.9-es lemma alapján nagyon nagy valószínűséggel

$$|L'| \le E(L') + (|L|a(L))^{1/2} \log^5 q \le$$

$$\le i b_{i+1} q^{1/2} + i \log^{22} q + |L|^{1/2} \log^{9\frac{1}{2}} q. \tag{5.11}$$

A bizonyítás befejezéséhez tehát csak azt kell megmutatnunk, hogy nagyon nagy valószínűséggel

$$|B_i(X)| \le o(b_{i+1} q^{1/2}) + \log^9 q, \tag{5.12}$$

$$|A_i(X') \cap B_i(X \setminus X')| \leq o(b_{i+1}q^{1/2}) + \log^9 q \tag{5.13}$$

minden X'-re. Tegyük fel, hogy az 5.12-es és az 5.13-as teljesül. Ekkor az 5.11-es alapján a bizonyítás teljessé tételéhez elég igazolni, hogy

$$|L|^{1/2}\log^{9\frac{1}{2}} q \leq (1-o(1))(b_{i+1}q^{1/2} + \log^{22} q).$$

Mindkét oldalt négyzetre emelve azt fogjuk belátni, hogy

$$|L|\log^{19} q \leq (1-o(1))(b_{i+1}^2 q + 2b_{i+1}q^{1/2}\log^{22} q + \log^{44} q).$$

Az indukciós hipotézis alapján $|L| \leq ib_iq^{1/2} + i\log^{22} q$, így

$$|L|\log^{19} q \leq ib_iq^{1/2}\log^{19} q + i\log^{41} q.$$

Mivel $i \ll \log^3 q$, ezért $i\log^{41} q \ll \log^{44} q$. Továbbá $b_{i+1} \geq b_i/2$, ezért $ib_iq^{1/2}\log^{19} q \ll b_{i+1}q^{1/2}\log^3 q \log^{19} q = b_{i+1}q^{1/2}\log^{22} q$, és ezzel beláttuk a fentit.
Így tehát már csak az 5.12-est és az 5.13-ast kell igazolnunk. Az elsőhöz vegyük észre, hogy az előző szakaszban használt érveléshez hasonlóan

$$|B_i(X)| = |B_i(u,v,w)| \leq \sum_{x\in S_i}\sum_{j:[jux]} t_j \sum_{j':[j'vx]} t_{j'} \sum_{j'':[j''wx]} t_{j''} = Y.$$

Felhasználva hipotézisünk azon részét, miszerint $|S_i(l)| \sim b_iq \leq 2b_iq$ tetszőleges l-re, kapjuk, hogy

$$E_0(Y) \leq p_i^3|S_i|(\max_l |S_i(l)|)^3 \leq 2p_i^3(b_iq^2)(b_iq)^3 = 2\theta^3 b_i q^{1/2} = \alpha,$$

$$E_1(Y) \leq p_i^2(\max_l |S_i(l)|)^3 \leq 2p_i^2(b_iq)^3 = 2\theta^2 b_i = O(1),$$

$$E_2(Y) \leq p_i \max_l(|S_i(l)|) \leq 2p_i(b_iq) = 2\theta q^{-1/2} = O(1),$$

$$E_3(Y) = 1.$$

A 4.4-es lemma tehát, $\lambda = a\log^{4/3} q$ választással (ahol a egy kicsi pozitív konstans) a következőt adja:

$$|B_i(X)| \leq \alpha + \alpha^{1/2}\log^4 q.$$

Használjuk fel, hogy

$$\alpha + \alpha^{1/2}\log^4 q \leq 2\alpha + \log^8 q,$$

(némi átrendezés után a triviális $bc \leq b^2 + c^2$ egyenlőtlenséghez jutunk), valamint hogy $2\alpha = 4\theta^3 b_i q^{1/2} = o(b_{i+1}q^{1/2})$, lévén $\theta = o(1)$ és $b_{i+1} \leq b_i/2$. Ezekből együttesen már következik az 5.12-es, az 5.13-as bizonyítása pedig hasonlóan működik. ■

5.2. Megjegyzés Ha $a(L) \leq |L|\log^{-100}$-nal dolgozunk az 5.10-esben, az 5.11-es jobboldali tagja $ib_{i+1}q^{1/2} + i\log^{10} q + |L|\log^{-45} q$-ra változik. Mivel $|L|\log^{-45} q = o(b_{i+1}q^{1/2})$, ez nem befolyásolja a bizonyítás menetét.

5.1.8. (6)-os

$$|A_{i+1}(u,v)| \le (i+1)b_{i+1}q + (i+1)\log^{40} q$$

A **(7)**-es bizonyításához hasonlóan legyen $X = \{u,v\}$ Ω_i két tetszőleges u,v pontjára. Legyen $L = A_i(u,v)$ és $L' = L \cap S_{i+1}$. Tudjuk:

$$|A_{i+1}(X)| \le |L'| + |B_i(X)| + \sum_{X' \subset X} |A_i(X') \cap B_i(X \setminus X')|, \tag{5.14}$$

ahol az utolsó összeget szokás szerint X összes megfelelő X' részhalmazára vesszük. Mivel S_i bármely pontja $1 - P_i^u$ valószínűséggel él túl,

$$E(|L'|) \le \left(ib_iq + i\log^4 0q\right)(1 - P_i^u) \le ib_{i+1}q + i\log^{40} q.$$

Másrészt a **(7)**-es miatt (lásd még a 4.9-es lemmát követő megjegyzést)

$$a(L) \le \max_{z \in \Omega_i} |A_i(u,v,w)| \le ib_iq^{1/2} + i\log^{22} q. \tag{5.15}$$

Ezért a 4.9-es lemma alapján nagyon nagy valószínűséggel

$$|L'| \le E(L') + (|L|a(L))^{1/2}\log^5 q \le$$

$$\le ib_{i+1}q + i\log^{40} q + |L|^{1/2}(ib_iq^{1/2} + i\log^{22} q)^{1/2}\log^5 q. \tag{5.16}$$

Az előző bizonyításnál látottakhoz hasonlóan megmutatható, hogy minden X'-re

$$|B_i(X)| \le o(b_{i+1}q) + \log^{39} q, \tag{5.17}$$

$$|A_i(X') \cap B_i(X \setminus X')| \le o(b_{i+1}q) + \log^{39} q, \tag{5.18}$$

e két egyenlőtlenség bizonyítását így most elhagyjuk. Utolsó lépésként elegendő megmutatni, hogy

$$|L|^{1/2}(ib_iq^{1/2} + i\log^{22} q)^{1/2}\log^5 q \le (1 - o(1))(b_{i+1}q + \log^{40} q).$$

Mindkét oldalt négyzetre emelve a következőt fogjuk igazolni:

$$|L|(ib_iq^{1/2} + i\log^{22} q)\log^{10} q \le (1 - o(1))(b_{i+1}^2q^2 + 2b_{i+1}q\log^{40} q + \log^{80} q).$$

Az indukciós hipotézis szerint

$$|L| \le ib_iq + i\log^{40} q \ll b_iq\log^3 q, \tag{5.19}$$

ahol ismételten kihasználtuk, hogy $i \ll \log^3 q$ és ebben a fázisban $b_iq \ge \log^{100} q$. Így

$$|L|(ib_iq^{1/2} + i\log^{22} q)\log^{10} q \le b_iqib_iq^{1/2}\log^{13} q + b_iqi\log^{35} q.$$

Használjuk ki ismét i nagyságrendjét, valamint hogy $b_{i+1} \ge b_i/2$ és $q^{1/2} \ge \log^{100} q$ (mindig feltesszük, hogy q kellően nagy), így igen tág becsléssel a következőkhöz jutunk:

$$b_iqib_iq^{1/2}\log^{13} q \le b_{i+1}^2q^2,$$

$$ib_iq\log^{35} q \le b_{i+1}q\log^{40} q,$$

teljessé téve ezzel a bizonyítást. ■

5.3. Megjegyzés Vegyük észre, hogy az előző bizonyítás során csupán egyetlen helyen, az 5.19-esben használtuk ki, hogy az algoritmus első fázisában vagyunk – egy alkalmas hibatag bevezetésével a bizonyítás és így a **(6)**-os tulajdonság átmenthető a második fázisba is, mégpedig $|A_i(u,v)| \le \log^{O(1)} q$ alakú becslés formájában. Vizsgáljuk meg most ezt. Abban az esetben, ha a második fázisban vagyunk, az 5.19-es a következőképpen módosul:

$$|L| \le ib_iq + i\log^{40} q \ll \log^3 qb_iq + \log^{43} q,$$

és itt fontos figyelnünk arra, hogy míg az első fázisban a jobboldal első tagja dominált, addig a második fázisban ez egyáltalán nem biztos, sőt ha q-t növeljük, előbb-utóbb a második tag lesz domináns. Így a becslés mindkét tagját meg kell hagynunk, és ezzel kell tovább számolnunk. Hasonlóan a fenti bizonyításhoz,

$$|L|(ib_iq^{1/2} + i\log^{22} q)\log^{10} q \le \log^{16} qb_i^2q^{3/2} + \log^{38} qb_iq + \log^{56} qb_iq^{1/2} + \log^{78} q.$$

Ha q megfelelően nagy, $\log^{16} qb_i^2q^{3/2} \le b_{i+1}^2q^2$, $\log^{38} qb_iq \le b_{i+1}q\log^{40} q$ és $\log^{56} qb_iq^{1/2} \le b_{i+1}q\log^{40} q$, ezért az eredeti állítás egy plusz $\log^{78} q$-s hibataggal érvényben marad.

5.2. Második fázis

Az **(1)**-es tulajdonság igazolása ugyanúgy történik, mint az előző fázisban. A **(4)**-es és **(5)**-ös tulajdonságok bizonyítása teljes egészében a 4.9-es lemmára épül és többé-kevésbé hasonló. A fázis nehézségét a **(2)**-es és **(3)**-as igazolása okozza, melyek meglehetősen technikásak.

5.2.1. (4)-es és (5)-ös

(4) $(1-\log^{-10} q)^{i+1}b_{i+1}q^2 \le |S_{i+1}| \le (1+\log^{-10} q)^{i+1}b_{i+1}q^2$

(5) $|\Omega_{i+1}| \le (1+\log^{-10} q)^{i+1}q^2b'_{i+1}$

Tekintsük az **(5)**-ös tulajdonságot. Szokás szerint legyen $L = \Omega_i$ és $L' = \Omega_{i+1}$. Vegyük észre, hogy az első fázis második tulajdonságából és $b'_i/b_i \le$ 2-ből (ami az indukciós hipotézis következménye, lásd például az 1.2-es tétel bizonyításánál) következik, hogy $|\Omega_i(l)| \le K\log^{c_1} q$ valamely K konstansra a második fázis minden lépése során. Emiatt $a(L) \le 2K\log^{c_1} qa_iq^{1/2}$. Másrészt $|L| \sim b_iq^2 \ge \frac{1}{2}b_iq^2 \ge \frac{1}{2}(\log^c q)q^{1/2}$ miatt $|L| \ge a(L)\log^{100} q$. A 4.9-es lemma alapján pedig nagyon nagy valószínűséggel

$$\big||L'| - E(|L'|)\big| \le (a(L)|L|)^{1/2}\log^5 q.$$

Felidézve, hogy $E(|L'|) \le L(1-P_i^u)$, kapjuk, hogy nagyon nagy valószínűséggel

$$|\Omega_{i+1}| = |L'| \le (1-P_i^l)|L| + (a(L)|L|)^{1/2}\log^5 q =$$

$$= |L| \left(1 - P_i^l + \left(\frac{a(L)}{|L|}\right)^{1/2}\right) \log^5 q.$$

Mivel a korábbiak alapján $\left(\frac{a(L)}{|L|}\right)^{1/2} \log^5 q \leq \log^{-20} q$, így

$$|L| \left(1 - P_i^l + \left(\frac{a(L)}{|L|}\right)^{1/2}\right) \log^5 q \leq |L|(1 - P_i^l)(1 + \log^{-10} q),$$

amivel beláttuk az **(5)**-öst. A **(4)**-es bizonyítása hasonló elven működik. ■

5.2.2. (2)-es

$$\tfrac{1}{2} b_{i+1}^2 q^3 (1 - 3(i+1)\log^{-13} q) \leq |T_{i+1}(v)| \leq \tfrac{1}{2} b_{i+1}^2 q^3 (1 + 3(i+1)\log^{-13} q)$$

A **(2)**-es bizonyításához először $|T_{i+1}(v)|$ várható értékét kell megbecsülnünk. Ebbe beletartozik annak az eseménynek várható értéke is, hogy egy (x, y) pár túlél S_{i+1}-ben. A gond csak az, hogy ha x és y két S_i-beli pont, akkor az $x \in S_{i+1}$, $y \in S_{i+1}$ események nem függetlenek. A következő lemma segít felülkerekedni ezen a problémán azáltal, hogy kimondja: a két esemény bizonyos értelemben majdnem független, ezért a kívánt várható érték megfelelő pontossággal számolható. E szakasz erejéig legyen $\delta = \log^{-13} q$.

5.4. Lemma *Bármely $x, y \in S_i$ pontra*

$$|P(x, y \in S_{i+1}) - P(x \in S_{i+1})P(y \in S_{i+1})| = o(\delta).$$

A lemma bizonyítása lényegében a szita-formula többszöri alkalmazásának segítségével történik, ennek ellenére meglehetősen komplikált levezetésről van szó, amely így helyhiány miatt elmarad (az eredeti bizonyítás [7] 350–354. oldalán olvasható). Nézzük tehát a **(2)**-es igazolását a fenti lemma segítségével.
Mivel $\delta = \log^{-13} q$, elegendő megmutatni, hogy nagyon nagy valószínűséggel

$$\left| |T_{i+1}(v)| - \frac{1}{2} b_{i+1}^2 q^3 \right| \leq 3(i+1)\delta b_{i+1}^2 q^3.$$

Első lépésként becsüljük $E(|T_{i+1}(v)|)$-t: definíció szerint

$$E(|T_{i+1}(v)|) = \sum_{x,y \in S_i : [xyv]} P(x, y \in S_{i+1}).$$

Az 5.4-es lemma alapján

$$|T_i(v)|P(x \in S_{i+1})^2(1 - o(\delta)) \leq E(|T_{i+1}(v)|) \leq |T_i(v)|P(x \in S_{i+1})^2(1 + o(\delta)).$$

Emlékeztetőül, $b_i P(x \in S_{i+1}) = b_{i+1}$, így az indukciós hipotézis szerint

$$\frac{1}{2} b_{i+1}^2 q^3 (1 - 3i\delta)(1 - o(\delta)) \leq E(|T_{i+1}(v)|) \leq \frac{1}{2} b_{i+1}^2 q^3 (1 + 3i\delta)(1 + o(\delta)). \tag{5.20}$$

Ezért már csak azt kell belátnunk, hogy $|T_{i+1}(v)|$ erősen koncentrálódik a várható értéke körül, és ehhez megint csak a 4.9-es lemmát alkalmazhatjuk. Az egyszerűség kedvéért $T_i(v)$ helyett a következő multihalmazt tekintsük:

$$T_i'(v) = \left\{ x^{m(x)} \mid x \in S_i \setminus v \right\},$$

ahol $m(x) = (|(xv)| - 2)$ az x multiplicitása ($|(xv)|$ az x-re és v-re illeszkedő egyenes pontjainak száma – értelemszerűen már csak a túlélő pontokkal dolgozunk). Nyilvánvaló, hogy $|T_i'(v)| = 2|T_i(v)|$.
Következő lépésként (a 4.9-es lemma segítségével) belátjuk, hogy $|T_i'(v)|$ erősen koncentrált. Szokás szerint legyen $L = T_i'(v)$ és $L' = T_{i+1}'(v)$. $a(L)$ becsléséhez vegyük észre, hogy (az indukciós hipotézis felhasználásával) tetszőleges u és v pontra

$$|A_i(T_i'(v), u)| \leq |A_i(u)| \max_x m(x) \leq |A_i(u)| 2 \log^{c_1} q \leq 4 a_i b_i q^{3/2} \log^{c_1} q = \alpha.$$

Így $a(L) \leq \alpha$. Mivel $|L| = |T_i'(v)| \sim b_i^2 q^3 = \beta$, a 4.9-es lemma alapján nagyon nagy valószínűséggel

$$\big||L'| - E(|L'|)\big| \leq (\alpha\beta)^{1/2} \log^5 q. \tag{5.21}$$

Lévén $c_1 = 100$ és $a_i \leq \log q$ (lásd a 3.8-as megjegyzést), $(\alpha\beta)^{1/2} \log^5 q =$
$= (4 a_i b_i^3 q^{9/2} \log^{100} q)^{1/2} \log^5 q \leq (b_i q^{3/2})^{3/2} \log^{60} q$. Másrészt $b_i q^{3/2} \geq \log^c q$, ahol $c = 300$, és $b_{i+1} \geq 0,9 b_i$ (lásd a 3.8-as megjegyzésnél). Így tehát $(b_i q^{3/2})^{3/2} \log^{60} q = o(\delta b_{i+1}^2 q^3)$. Ebből az 5.20–5.21-es felhasználásával már (igen tág becsléssel) következik a **(2)**-es tulajdonság. ■

5.2.3. (3)-as

$$a_{i+1} b_{i+1} q^{3/2}(1 - O(i\theta^2)) \leq |A_{i+1}(v)| \leq a_{i+1} b_{i+1} q^{3/2}(1 + O(i\theta^2))$$

Az indukciós hipotézis alapján feltehető, hogy

$$a_i b_i q^{3/2}(1 - K(i-1)\theta^2) \leq |A_i(v)| \leq a_i b_i q^{3/2}(1 + K(i-1)\theta^2),$$

valamely 16-nál nagyobb K konstansra.
Legyen $U_i = B_i \setminus M_i$. Jelölje $U_i(v)$ ($B_i(v), M_i(v)$) azon $x \in S_i$ pontok halmazát, melyekhez létezik $u \neq x \in U_i$ (B_i, M_i), amire x, u és v egy egyenesre esik. Legyen továbbá $B_i'(v)$ és $M_i'(v)$ $B_i(v)$ és $M_i(v)$ S_{i+1}-el vett metszete.
Szokásosan jelölje L $A_i(v)$-t és $L' := L \cap S_{i+1}$. Mivel A_i és A_{i+1} ívek, ezért tetszőleges $v \in \Omega_{i+1}$ pontra

$$|A_{i+1}(v)| = |L'| + |M_i'(v)|.$$

Hasonlóan az eddigiekhez, könnyen megmutatható, hogy $|L'|$ kellően koncentrálódik a várható értéke körül. A bizonyítás nehezebb része $M_i'(v)$ becslésében rejlik.
A szakasz hátralevő részéhez legyen $\delta = \log^{-10} q$. Vegyük észre, hogy

$$|B_i'(v)| - |U_i(v)| \leq |M_i'(v)| \leq |B_i'(v)| \leq |B_i(v)|,$$

ennek segítségével fogjuk $M_i'(v)$-t becsülni. A következő három állítás a fenti észrevételben szereplő mennyiségek ($|B_i(v)|, |B_i'(v)|$,
$|U_i(v)|$) becslésére vonatkozik.

5.5. Állítás *Nagyon nagy valószínűséggel*

$$|B_i(v)| \leq \theta b_i q^{3/2}(1 + o(\delta)).$$

Bizonyítás: Definíció szerint egy x pont akkor van $B_i(v)$-ben, ha létezik olyan $j \in (xv)$, melyre $j \in B_i$, azaz $t_j = 1$. Ezért

$$|B_i(v)| \leq \sum_{x \in S_i} \left(\sum_{j:[jxv]} t_j \right). \tag{5.22}$$

A kettős szummában minden t_j pontosan m_j-szer szerepel, ahol m_j a (vj) egyenes túlélő pontjainak száma (leszámítva v-t és j-t). Ezért az 5.22-es jobboldala a következő formába írható: $\sum_{x \in S_i} t_x m(x) = Y$. Y becsléséhez a 4.5-ös következményt fogjuk használni. Vegyük észre, hogy $\sum_{x \in S_i} m(x)$ éppen az előző szakaszban definiált $|T_i'(v)| = 2|T_i(v)|$ mennyiség. Így

$$E_0(Y) = 2p_i|T_i(v)| \sim p_i b_i^2 q^3(1 + o(\delta)) \sim \theta b_i q^{3/2} \geq \log^{150} q, \tag{5.23}$$

lévén $b_i q^{3/2} \geq \log^{300} q$, valamint felhasználtuk $|T_i(v)|$ **(2)**-es tulajdonságbeli becslését is. Továbbá amikor belépünk a második fázisba, minden egyenesnek nagyjából $\log^{c_1} q = \log^{100} q$ túlélő pontja van, éppen ezért

$$E_1(Y) \leq \max_x m(x) \leq \max_l |S_i(l)| \leq 2 \log^{c_1} q.$$

Így a 4.5-ös következmény alapján nagyon nagy valószínűséggel

$$|B_i(v)| \leq E_0(Y)(1 + o(\delta)).$$

Ebből az 5.23-assal együtt kapjuk, hogy $|B_i(v)| \leq \theta b_i q^{3/2}(1 + o(\delta))$. ■

5.6. Állítás *Nagyon nagy valószínűséggel*

$$|B_i'(v)| \geq \theta b_i q^{3/2}(1 - o(\delta)) - 8a_i \theta^2 b_i q^{3/2}.$$

Bizonyítás: Vegyük észre, hogy egy x pont éppen akkor $B_i'(v)$-beli, ha $x \in S_{i+1}$ és létezik legalább egy (x-től és v-től különböző) B_i-be tartozó pont az (xv) egyenesen. Jelöljük $B_i''(v)$-vel azon $x \in S_{i+1}$ pontok halmazát, melyekhez pontosan egy (xv)-re eső pont van a fenti tulajdonsággal. Nyilvánvaló, hogy $|B_i'(v)| \geq |B_i''(v)|$. Azt fogjuk belátni, hogy már $|B_i''(v)|$-re is teljesül az állítás. A trükk ebben az, hogy míg a megszorítások $B_i''(v)$-t könnyebben kezelhetővé teszik, mégsem vesztünk túl sok pontot, mivel annak valószínűsége, hogy B_i több mint egy pontban metsz egy egyenest, elhanyagolható. $|B_i''(v)|$-t a szokásos módon polinommal tudjuk becsülni a következőképpen:

$$|B_i''(v)| \geq \sum_{x \in S_i : |(xv)| \geq 3} \mathbf{1}_{x \in S_{i+1}} \sum_{j:[jxv]} t_j \left(1 - \sum_{j' \neq j:[j'xv]} t_{j'}\right), \tag{5.24}$$

ahol $|(xv)| \geq 3$ azt jelenti, hogy az (xv) egyenesnek (x-et és v-t beleértve) legalább három túlélő pontja van. Az egyenlőtlenség jobboldala tovább alakítható, ha figyelembe vesszük egy pont törléséhez vezető okokat:

$$\mathbf{1}_{\{x \in S_{i+1}\}} \geq 1 - \left(\sum_{g \in A_i(x)} t_g + \sum_{g,g':[gg'x]} t_g t_{g'} \right).$$

Így

$$|B_i''(v)| \geq$$

$$\geq \sum_{x \in S_i : |(xv)| \geq 2} \left(1 - \left(\sum_{g \in A_i(x)} t_g + \sum_{g,g':[gg'x]} t_g t_{g'} \right)\right) \left(\sum_{j:[jxv]} t_j \left(1 - \sum_{j' \neq j:[j'xv]} t_{j'}\right)\right).$$

A következő lépésben elvégezzük a szorzásokat és a jobboldalt két tag összegére bontjuk, ahol a fő tag $\sum_{x:|(xv)|\geq 2} \sum_{j:[jxv]} t_j$, és a hibatagba kerül minden más. Az 5.5-ös állítás igazolásához hasonlóan megmutatható, hogy a fő tag nagyon nagy valószínűséggel legalább $\theta b_i q^{3/2}(1 - o(\delta))$. A 4.4-es lemma alkalmazásával pedig belátható, hogy a hibatag legalább $-8a_i\theta^2 b_i q^{3/2}$. Ezeket a sok technikai részletet igénylő, de alapjában véve egyszerű számításokat mellőzzük. ■

5.7. Állítás *Nagyon nagy valószínűséggel*

$$|U_i(v)| \leq 6\theta^2 a_i b_i q^{3/2}.$$

Bizonyítás: Vegyük észre, hogy bármely $x \in U_i(v)$ ponthoz kell legyen olyan x-től és v-től különböző $j \in (xv)$ pont, melyre $j \in B_i$, de $j \notin M_i$. Ezért

$$|U_i(v)| \leq \sum_{x:|(xv)|\geq 3} \sum_{j:[jxv]} t_j \mathbf{1}_{\{j \notin M_i\}}.$$

Az algoritmus leírása alapján két ok van, mely kizárja j-t M_i-ből: vagy vannak olyan j' és j'' pontok B_i-ben, hogy j, j' és j'' egy egyenesre esnek; vagy létezik olyan $j' \in B_i$, melyre

(jj') metszi A_i-t. Így

$$\sum_{x:|(xv)|\geq 3}\sum_{j:[jxv]} t_j \mathbf{1}_{\{j\notin M_i\}} \leq \sum_{x:|(xv)|\geq 3}\sum_{j:[jxv]} t_j \left(\sum_{j',j'':[jj'j'']} t_{j'}t_{j''} + \sum_{j'\in A_i(j)} t_{j'}\right).$$

Vágjuk a jobboldalt két részre, α-ra és β-ra, ahol

$$\alpha = \sum_{x:|(xv)|\geq 2}\sum_{j:[jxv]} t_j \left(\sum_{j',j'':[jj'j'']} t_{j'}t_{j''}\right),$$

$$\beta = \sum_{x:|(xv)|\geq 2}\sum_{j:[jxv]} t_j \left(\sum_{j'\in A_i(j)} t_{j'}\right).$$

A 4.4-es lemma használatával aránylag egyszerű megmutatni, hogy nagyon nagy valószínűséggel $\alpha \leq 5\theta^3 b_i q^{3/2} = o(\theta^2 a_i b_i q^{3/2})$ és $\beta \leq 5\theta^2 a_i b_i q^{3/2}$. Az állítás ezekből azonnal következik. ■

5.8. Állítás *Ha az algoritmus az $i-1$-edik lépésig tökéletesen fut, akkor $b_i/b_{i+1} \leq 1+2\theta a_i$.*

Bizonyítás: Definíció szerint

$$\frac{b_i}{b_{i+1}} = \frac{1}{1-P_i^u} = \frac{1}{1-p_i \max_v |A_i(v)|(1+o(1))},$$

ahol az utolsó átalakítás során felhasználtuk a 3.2-es lemmát (vegyük észre, hogy ebben a lemmában $p_i \max_v |A_i(v)|$ a felső becslés domináns tagja). Mivel az indukciós hipotézis szerint $|A_i(v)| \sim a_i b_i q^{3/2} \leq \frac{3}{2} a_i b_i q^{3/2}$, ezért

$$p_i \max_v |A_i(v)| \leq \theta (b_i q^{3/2})^{-1} \frac{3}{2} a_i b_i q^{3/2} \leq \frac{3}{2}\theta a_i.$$

Emiatt

$$\frac{1}{1-p_i \max_v |A_i(v)|(1+o(1))} \leq 1 + 2\theta a_i,$$

lévén $\theta a_i = o(1)$. ■

A fenti állítások ismeretében már készen állunk $|M_i'(v)|$ becslésére. Az 5.5-ös és 5.8-as állítások alapján nagyon nagy valószínűséggel

$$|M_i'(v)| \leq |B_i(v)| \leq \theta b_i q^{3/2}(1+o(\delta)) \leq$$

$$\leq \theta b_{i+1} q^{3/2}(1+2\theta a_i)(1+o(\delta)) \leq$$

$$\leq \theta b_{i+1} q^{3/2}(1+3\theta a_i). \tag{5.25}$$

Másrészt a második és harmadik állítás szerint

$$|M_i'(v)| \geq |B_i'(v)| - |U_i(v)| \geq \theta b_i q^{3/2}(1-o(\delta)) - 8\theta^2 a_i b_i q^{3/2} - 2\theta^2 a_i b_i q^{3/2} \geq$$

$$\geq \theta b_{i+1} q^{3/2}(1 - 15\theta a_i). \tag{5.26}$$

Az 5.25-ösben és az 5.26-osben kihasználtuk, hogy $\delta = \log^{-10} q \ll \theta a_i$, így az $o(\delta)$ hozzájárulását egy további θa_i tag dominálta.
Utolsó lépésként becsüljük $|L'|$-t. A 4.10-es következményt fogjuk használni, ehhez először $a(L)$-t kell becsülni. Mivel $L = A_i(v)$, ezért $a(L) = \max_{u,v} |A_i(u,v)|$, így az első fázis **(6)**-os tulajdonságára lesz szükségünk. Az 5.3-as megjegyzés értelmében tetszőleges u és v pontokra

$$|A_i(u,v)| \leq i b_i q + i \log^{40} q + \log^{78} q.$$

Tekintettel arra, hogy $i \leq N \leq \log^3 q$ és a második fázisban $b_i q \leq \log^{c_1} q = \log^{100} q$, ezért a fentiből $a(L) \leq \log^{103} q$ következik.
Mivel

$$E(|L'|) \sim a_i b_{i+1} q^{3/2} \geq a_i \log^c q = a_i \log^{300} q \geq \log^{298} q,$$

a 4.10-es következményből fakadóan nagyon nagy valószínűséggel

$$a_i b_{i+1} q^{3/2}(1 - K(i-1)\theta^2)(1 - o(\delta)) \leq |L'| \leq$$

$$\leq a_i b_{i+1} q^{3/2}(1 + K(i-1)\theta^2)(1 + o(\delta)). \tag{5.27}$$

$|L'|$ várható értéke $a_i b_{i+1} q^{3/2}(1 \pm K(i-1)\theta^2)$ között korlátozódik, $o(\delta)$ a szórás farkából származó hibatag. Az 5.26-osból és az 5.27-esből tehát nagyon nagy valószínűséggel

$$|A_{i+1}(v)| = |L'| + |M_i'(v)| \geq$$

$$\geq a_i b_{i+1} q^{3/2}(1 - K(i-1)\theta^2)(1 - o(\delta)) + \theta b_{i+1} q^{3/2}(1 - 15\theta a_i) \geq$$

$$\geq b_{i+1} q^{3/2}(a_i + \theta - K a_i i \theta^2 - 15 a_i \theta^2) \geq$$

$$\geq b_{i+1} q^{3/2}(a_{i+1} - \theta^3 - K a_i i \theta^2 - 15 a_i \theta^2).$$

A második egyenlőtlenségben a $K a_i i$ és $K a_i (i-1)$ közti különbség lenyeli az $o(\delta)$-s hibatagot. A harmadik egyenlőtlenséghez felhasználtuk, hogy $a_{i+1} \leq a_i + \theta + \theta^3$ (lásd az 5.1-es megjegyzést). Mivel $a_{i+1} \geq a_i$ és $K \geq 16$, a fentiek alapján

$$|A_{i+1}(v)| \geq a_{i+1} b_{i+1} q^{3/2}(1 - K(i+1)\theta^2).$$

A felső becsléshez az 5.25-ösből és az 5.27-esből következik, hogy

$$|A_{i+1}(v)| \leq a_i b_{i+1} q^{3/2}(1 + K(i-1)\theta^2)(1 + o(\delta)) + \theta b_{i+1} q^{3/2}(1 + 3\theta a_i) \leq$$

$$\leq b_{i+1} q^{3/2}(a_i + \theta + K a_i i \theta^2 + 3 a_i \theta^2).$$

Ismét vegyük észre, hogy az i és $i-1$ közti különbség lenyeli $o(\delta)$ hozzájárulását. Az 5.1-es megjegyzés szerint

$$a_{i+1} \geq a_i + \theta - (3a_i\theta^2 + 10\theta^3) \geq a_i + \theta - 4a_i\theta^2,$$

és ez alapján

$$|A_{i+1}(v)| \leq a_{i+1}b_{i+1}q^{3/2}(1 + Ki\theta^2 + 7\theta^2) \leq$$

$$\leq a_{i+1}b_{i+1}q^{3/2}(1 + K(i+1)\theta^2).$$

■

Összefoglalás

Az előző fejezetek során megismerkedhettünk a valószínűségi módszer elvével, a projektív síkok alapvető tulajdonságaival, az ívek fogalmával és történetével, valamint erős koncentrációs eredményekkel. Ami összefogta ezeket a meglehetősen széles skálán mozgó területeket, az a következő kérdés volt: egy q-rendű projektív síkon legfeljebb mekkora lehet a legkisebb teljes ív mérete? Bár ez a probléma alapvetően a véges geometria tárgykörébe tartozik, az elmúlt 40 év talán legjelentősebb áttörése a kérdés megválaszolásában mégis Kim és Van tétele, melyet a valószínűségszámítás eszközeit felhasználva bizonyítottak. Eszerint a keresett mennyiség $\sqrt{q}\log^c q$-val felülről becsülhető – ami a korábbról már ismert $\sqrt{2q}$-s alsó határral együtt egy polilogaritmikus faktor erejéig meghatározza a kérdéses ív méretét.

A fő tétel bizonyításához bevezettük a dinamikus véletlen konstrukció módszerét, majd ismertettünk egy erre alapuló algoritmust, és azt állítottuk, hogy ennek végeredményeként igen nagy valószínűséggel épp a kívánt méretű teljes ívet kapjuk. Az algoritmus során kulcsfontosságú tényező volt, hogy bizonyos paraméterek – úgy mint a túlélő pontok száma egy egyenesen, a rendelkezésre álló ponthalmaz mérete stb. – értékét adott korlátok közé tudjuk szorítani. Számos esetben pontosan arra volt szükség, hogy ezek a véletlen változók a várható értékeik körül koncentrálódjanak. Megmutattuk, hogy az eljárásunk komplexitása miatt ennek igazolására a klasszikus eszközök, úgy mint az Azuma- vagy Talagrand-egyenlőtlenség nem alkalmasak, éppen ezért új koncentrációs eredmény bevezetésére volt szükségünk. Ehhez definiáltuk, hogy mit értünk egyáltalán erős koncentráción, és bemutattuk, hogyan lehet a klasszikus eszközöket úgy megjavítani, hogy esetünkben is alkalmazható eredményt nyerjünk. Mindezt egy egyszerű példán is szemléltettük. Végül az új koncentrációs eredmény segítségével igazoltuk a paramétereink megfelelő viselkedését. Az eredmények igazolása során láthattuk, milyen nagy szerepe van a paraméterek és a szükséges koncentrációs eszközök helyes megválasztásának, ennek segítségével ugyanis az eredetileg legnehezebbnek ígérkező rész, a véletlen változók kezelése egyszerű számításokká redukálódott.

Szakdolgozatom célja az algoritmus síkbeli működésének bemutatása volt, érdekes kérdés lehet azonban, hogy vajon mi a helyzet projektív terek esetén? Három dimenzióban kétféle természetes kiterjesztési lehetőség adódik: az egyik szerint ívnek immár azon ponthalmazokat nevezzük, melyeknek semelyik négy pontja nem esik egy síkba (emlékeztetőül,

két dimenzióban semelyik három pont nem eshetett egy egyenesre); a másik megközelítés változatlanul hagyja az ív síkbeli definícióját, csak immár térre áttérve – ezeket a ponthalmazokat, hogy az első megközelítéstől megkülönböztessük, *süveg*nek nevezzük. Előzetes vizsgálataim alapján úgy tűnik, hogy a dolgozatom során bemutatott eljárás a paraméterek értelmes megválasztásával (és nyilvánvalóan az ív méretének változásával) átmenthető a süveg esetére, azonban a pontos állítás kimondása további kutatómunkát igényel. Az első megközelítés vizsgálata is sok lehetőséget rejt magában, ebben az esetben viszont nyilvánvalóan új paraméterekre lenne szükségünk, például a korábban igen nagy szerepet játszó, az egyeneseken levő túlélő pontok számát jelölő változónk helyett a síkbeli túlélő pontok számát kellene vizsgálnunk. A témakör tehát még koránt sincs lezárva, a síkbeli teljes ív lehető legkisebb méretének további pontosításától kezdve a térbeli, vagy akár magasabb dimenzióbeli eredmények elérése még mindig nyitott probléma.

Köszönetnyilvánítás

Dolgozatom nem jöhetett volna létre témavezetőm, Sziklai Péter nélkül, aki nemcsak a téma kiválasztásában, hanem annak feldolgozásában is nagy segítséget nyújtott, így elsősorban neki szeretnék köszönetet mondani. Nagyon hálás vagyok Fried Katalin tanárnőnek a Latex használatában nyújtott felbecsülhetetlen értékű segítségéért, a dolgozat végső formáját tanácsainak köszönhetem. Köszönettel tartozom továbbá Vu Ha Vannak, aki értékes megjegyzésével segített hozzá egy bizonyítás teljessé tételéhez.

Irodalomjegyzék

[1] N. Alon and J. Spencer. *The Probabilistic Method.* Wiley, New York, 1992.

[2] Noga Alon, J. H. Kim, and Joel Spencer. Nearly perfect matchings in regular simple hypergraphs. *Israel Journal of Mathematics*, 100:171–187, 1997.

[3] S. Ball. On small complete arcs in a finite plane. *Discrete Math*, 174:29–34, 1997.

[4] A. Blokhuis. Polynomials in finite geometry and combinatorics. *Survey in Combinatorics*, pages 35–52, 1993.

[5] J. C. Fisher. Random k-arcs, Preliminary report. 1989.

[6] J. H. Kim and V. H. Vu. Concentration of multivariate polynomials and its applications. *Combinatorica*, 20(3):417–434, 2000.

[7] J. H. Kim and V. H. Vu. Small complete arcs in projective planes. *Combinatorica*, 23(2):311–363, 2003.

[8] L. Lunelli and M. Sce. Considerazioni arithmetiche e risultati sperimentali sui $\{K; n\}_q$ archi. *Ist. Lombardo Accad. Sci. Rend. A*, 98:3–52, 1964.

[9] B. Segre. Le geometrie di Galois. *Ann. Mat. Pura Appl.*, 48:1–97, 1959.

[10] T. Szőnyi. Arcs, caps, codes and 3-independent subsets. *Giornate di Geometrie Combinatorie*, pages 57–80, 1993.

[11] M. Talagrand. A new look at independence. *The Annals of Probability*, 24:1–34, 1996.

[12] V. H. Vu. Concentration of non-Lipschitz functions and applications. *Random Structures and Algorithms*, 20:262–316, 2002.