Föreläsning 11: Probabilistiska metoden · 1MA020

Vilhelm Agdur[1]

[1] vilhelm.agdur@math.uu.se

16 mars 2023

I denna föreläsning ger vi fler tillämpningar av probabilistiska metoden på olika problem, praktiska och från andra delar av matematiken. Många men inte alla kommer handla om grafer.

`min-bisection`-problemet

Antag att vi har en grupp personer på en konferens, och vi vill dela upp dem i två lika stora grupper i olika rum. Vi vill att så många som möjligt som känner varandra skall få vara i samma rum – ekvivalent vill vi alltså minimera mängden vänskapsband mellan rummen.[2]

[2] Ett annat sätt att motivera det här problemet är att vi har en graf som är för stor för att lagra i minnet på en enda dator, så vi vill använda två datorer och låta var och en av dem lagra hälften. Så länge vad vi vill räkna ut bara handlar om noder på en av de två datorerna kan vi räkna lokalt – men om vi vill räkna ut något som involverar kanter mellan de två maskinerna måste de kommunicera med varandra, vilket är långsamt.

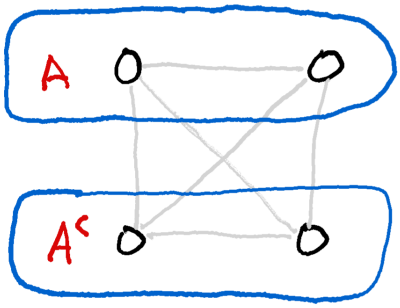
För att kunna göra snabba beräkningar vill vi alltså hitta ett sätt att dela upp vår graf så att det inte går så många kanter mellan de två delarna. Det här är ett problem som behöver lösas i praktiken, även om man ofta då har fler än två datorer och behöver hitta en minimal k-partition av grafen istället.

Definition 1. Givet en graf $G = (V, E)$ på $2n$ noder är `min-bisection` problemet att hitta en minimal bisektion av G, alltså att hitta en delmängd $A \in \binom{V}{n}$ som minimerar antalet kanter mellan A och A^c. Formellt skriver vi

$$\min_{A \in \binom{V}{n}} |E(A, A^c)|$$

där $E(A, A^c)$ alltså är mängden av kanter mellan A och dess komplement A^c.

Hur väl kan vi lösa det här problemet? Ibland är det väldigt svårt – om vi har fyra personer där alla känner alla, alltså grafen är den fullständiga grafen K_4, kommer vi alltid att ha 4 av 6 kanter mellan de två delarna.



Figur 1: K_4 uppdelad i en bisektion. På grund av symmetrin i grafen är detta så klart enda sättet att dela upp den.

Det visar sig att nyckelegenskapen för att kunna göra det här väl är att grafen inte får ha för många kanter relativt antalet noder – vilket väl inte är allt för överraskande, om man tänker efter.

För att kunna ge en precis variant av det påståendet behöver vi en definition och en sats från grafteorin.

Definition 2. En Hamiltoncykel i en graf är en cykel som innehåller alla noder exakt en gång. Givet $G = ([n], E)$ kan vi alltså se det som en permutation $\sigma \in S_n$ sådan att $\{\sigma(i), \sigma(i+1)\}$ är en kant för alla i, och $\{\sigma(1), \sigma(n)\} \in E$.

Teorem 3 (Diracs sats)**.** [3] *Om varje nod i $G = ([n], E)$ har grad*[4] *minst $\frac{n}{2}$ så finns det en Hamiltoncykel i G.*

[3] Inte fysikern, en annan Dirac.

[4] Antal grannar.

Bevis. Hade gärna inkluderat ett, men vi har inte riktigt tid med det – och hittade inget probabilistiskt bevis för detta, så det passar inte helt. □

Vi kan använda denna sats för att bevisa följande resultat:

Proposition 4. *Låt $G = ([n], E)$ vara en graf på ett jämnt antal noder, och antag att varje nod har grad högst $\frac{n}{2}$. Då existerar det en delmängd $A \in \binom{[n]}{n/2}$ sådan att*

$$E(A, A^c) \leq \frac{|E|}{2}.$$

Bevis. Låt G' vara komplementgrafen till G – alltså grafen där det finns en kant mellan varje par av noder som *inte* har en kant mellan sig i G, och som inte har en kant mellan par av noder som har en kant i G.

Vi ser enkelt att graden av i i G' är precis n minus graden av i i G, så eftersom $d_i \leq n/2$ i G måste $d'_i \geq n/2$ i G'. Alltså kan vi tillämpa Diracs sats och hitta en Hamiltoncykel σ i komplementgrafen G'.

Vi kan nu använda denna Hamiltoncykel för att para ihop noder i G – vi matchar $\sigma(1)$ med $\sigma(2)$, $\sigma(3)$ med $\sigma(4)$, och så vidare. Eftersom detta var en Hamiltoncykel i komplementgrafen är vi alltså garanterade att vi aldrig parar ihop två noder som har en kant mellan sig.

Vi kan nu skapa oss en slumpmässig delmängd $A \in \binom{[n]}{n/2}$ genom att, för varje par, slumpmässigt välja en av de två noderna att ha med i A, och låta den andra vara utanför A. Denna delmängd kommer ha rätt storlek eftersom vi väljer en nod ur varje par, så vi måste få precis hälften av noderna.

Låt oss nu räkna ut väntevärdet av $E(A, A^c)$. Vi får att

$$\begin{aligned}
\mathbb{E}\left[E(A, A^c)\right] &= \mathbb{E}\left[\sum_{e \in E} \mathbb{1}_{\{e \in E(A, A^c)\}}\right] \\
&= \sum_{e \in E} \mathbb{E}\left[\mathbb{1}_{\{e \in E(A, A^c)\}}\right] \\
&= \sum_{e \in E} \mathbb{P}\left(e \in E(A, A^c)\right).
\end{aligned}$$

Vad är sannolikheten att en viss fix kant $e = \{u, v\}$ går mellan A och A^c? Jo, det händer precis när vi valt att $u \in A$ och $v \in A^c$, eller

vice versa. Så vi kan räkna att[5]

$$\mathbb{P}\left(\{u,v\} \in E(A,A^c)\right) = \mathbb{P}\left(u \in A, v \in A^c\right) + \mathbb{P}\left(u \in A^c, v \in A\right).$$

[5] Vi utnyttjar att de är disjunkta händelser för att gå från $\mathbb{P}\left((u \in A, v \in A^c) \cup (u \in A^c, v \in A)\right)$ till summan av de två sannolikheterna.

Nyckeln nu, och anledningen att vi krånglade med Hamiltoncykeln och hopparningen, är att händelserna $u \in A$ och $v \in A^c$ måste vara oberoende. Om u är i A eller inte beror på en myntsingling vi gjorde för u och noden den parades ihop med – så om vi kallar dess partner för w så är $u \in A$ och $w \in A$ inte oberoende, men för alla $v \neq w$ är $u \in A$ oberoende från $v \in A$.

Så hur vet vi att vårt par u, v i vår räkning inte råkar vara hopparade, så att det inte är oberoende ifall de ligger i A eller ej? Jo, vi vet ju att det går en kant mellan u och v – det är därför vi är intresserade av dem – men det går ingen kant mellan något par av hopparade noder.

Alltså kan vi fortsätta vår räkning och få

$$\begin{aligned}\mathbb{P}\left(\{u,v\} \in E(A,A^c)\right) &= \mathbb{P}\left(u \in A, v \in A^c\right) + \mathbb{P}\left(u \in A^c, v \in A\right)\\ &= \mathbb{P}\left(u \in A\right)\mathbb{P}\left(v \in A^c\right) + \mathbb{P}\left(u \in A^c\right)\mathbb{P}\left(v \in A\right)\\ &= \frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{2}\end{aligned}$$

och alltså har vi att

$$\begin{aligned}\mathbb{E}\left[E(A,A^c)\right] &= \sum_{e\in E}\mathbb{P}\left(e \in E(A,A^c)\right)\\ &= \sum_{e\in E}\frac{1}{2} = \frac{|E|}{2}.\end{aligned}$$

Enligt vårt sedvanliga argument att väntevärdet omöjligen kan vara mindre än varje specifikt utfall måste det alltså finnas ett specifikt A sådant att $E(A,A^c) \leq \mathbb{E}\left[E(A,A^c)\right] = \frac{|E|}{2}$ och vi har bevisat satsen. □

ACNSL-olikheten och VLSI

I nästan varje sak vi gjort som involverat grafer så har vi ritat bilder av grafen på tavlan, och försökt göra dessa bilder så tydliga som möjligt. Vi väljer att rita dem så att kanterna inte korsar varandra om de inte absolut måste.

Detta leder oss till en faktisk matematisk fråga: Givet en graf G, hur få korsningar mellan kanter kan vi rita den med?

Definition 5. En graf G som vi kan rita helt utan att några kanter korsar varandra kallas för *planär*. I allmänhet betecknar vi det minimala antalet korsningar av kanter i en ritning av G med $cr(G)$.[6]

[6] Från engelskans *crossing number*.

Låt oss återigen ge ett lemma som vi inte bevisar.

Lemma 6. *Det gäller för alla grafer $G = (V,E)$ att*

$$cr(G) \geq |E| - 3|V| + 6.$$

Bevis. Utelämnas.[7] □

Anledningen att vi ger den här olikheten är att vi faktiskt kan enkelt härleda en starkare version av samma olikhet med ett probabilistiskt trick. Såsom mycket annan modern matematik är listan av upptäckare lång – till skillnad från förr i tiden görs merparten av all matematik i samarbeten numera.

Teorem 8 (Ajtai-Chvatal-Newborn-Szemerédi-Leighton (ACNSL))**.** *För varje graf $G = (V, E)$ gäller det att, om $|E| \geq 4|V|$ så är*

$$cr(G) \geq \frac{|E|^3}{64|V|^2}.$$

Bevis. För att förenkla vår notation, låt $n = |V|$ och $e = |E|$. Tag ett godtyckligt $p \in (0, 1)$.

Vad vi vill göra är att studera en slumpmässig delgraf H till G, som ges av att varje nod i G är med i H med sannolikhet p, och varje kant är med om bägge dess ändpunkter är med i H.[8]

Vi får av Lemma 6 att

$$cr(H) \geq |E(H)| - 3|V(H)| + 6.$$

Eftersom denna likhet gäller för *alla* utfall måste den också gälla om vi tar väntevärdet på bägge sidorna,[9] så från väntevärdets linjäritet får vi alltså att

$$\mathbb{E}\left[cr(H)\right] \geq \mathbb{E}\left[|E(H)|\right] - 3\mathbb{E}\left[|V(H)|\right] + 6. \tag{1}$$

Så låt oss studera vardera av dessa väntevärden. Så vi räknar att

$$\begin{aligned}\mathbb{E}\left[|V(H)|\right] &= \mathbb{E}\left[\sum_{v \in V(G)} \mathbb{1}_{\{v \in V(H)\}}\right] \\ &= \sum_{v \in V(G)} \mathbb{P}\left(v \in V(H)\right) = |V(G)|p = np,\end{aligned}$$

och

$$\begin{aligned}\mathbb{E}\left[|E(H)|\right] &= \mathbb{E}\left[\sum_{\{u,v\} \in E(G)} \mathbb{1}_{\{\{u,v\} \in E(H)\}}\right] \\ &= \sum_{\{u,v\} \in E(G)} \mathbb{P}\left(\{u, v\} \in E(H)\right) \\ &= \sum_{\{u,v\} \in E(G)} \mathbb{P}\left(u \in V(H), v \in V(H)\right) \\ &= \sum_{\{u,v\} \in E(G)} \mathbb{P}\left(u \in V(H)\right)\mathbb{P}\left(v \in V(H)\right) = |E(G)|p^2 = ep^2.\end{aligned}$$

[7] Idén i beviset är att använda Eulers formel och sedan resonera om att ta bort kanter som korsar andra kanter:

Lemma 7 (Eulers formel)**.** *Om $G = (V, E)$ är planär är*

$$3|V| - 6 \geq |E|.$$

Hur bevisar man Eulers formel? Den är ett specialfall av Eulerkarakteristiken av en polyeder. För en väldigt lång och intressant diskussion av just hur man bevisar detta, och primärt vad det faktiskt innebär att bevisa något, se Imre Lakatos bok *Proofs and Refutations*, som handlar enbart om just det.

[8] Detta kallas i allmänhet *nodperkolation* på G. Perkolationsteori är ett stort ämne i sannolikhetsteorin, med kopplingar till fysiken – man brukar tänka sig det som en modell för hur vatten sipprar genom sten. Således namnlikheten till perkolatorkaffe.

[9] Vi kan formulera detta som ett lemma:

Lemma 9. *Om $X(\omega) \geq Y(\omega)$ för varje $\omega \in \Omega$ så är $\mathbb{E}[X] \geq \mathbb{E}[Y]$.*

Bevis. Vi räknar att

$$\begin{aligned}\mathbb{E}[X] &= \sum_{\omega \in \Omega} X(\omega)\mu(\omega) \\ &\geq \sum_{\omega \in \Omega} Y(\omega)\mu(\omega) = \mathbb{E}[Y].\end{aligned}$$

□

Hur hanterar vi $\mathbb{E}[cr(H)]$? Jo, vi tar en ritning av G som har precis $cr(G)$ korsningar, och räknar hur många av de korsningarna som är kvar när vi suddat ut alla noder och kanter utanför H.

För att korsningen skall vara kvar krävs det så klart att bägge kanterna i korsningen är kvar – och vi har sett att sannolikheten att en enda kant är kvar är p^2, så eftersom kanter är kvar oberoende av varandra[10] är sannolikheten att en korsning blir kvar p^4.

Så enligt samma logik som i de andra fallen får vi att $\mathbb{E}[cr(H)] = cr(G)p^4$, så om vi sätter in resultatet av våra räkningar i (1) så får vi att

$$p^3 cr(G) \geq p^2 e - 3pn + 6$$

så om vi nu väljer $p = \frac{4n}{e}$ så får vi alltså

$$\left(\frac{4n}{e}\right)^3 cr(G) \geq \frac{(4n)^2}{e} - 3\frac{4n^2}{e} + 6 > \frac{(4n)^2}{e} - 3\frac{4n^2}{e}$$

vilket förenklar till påståendet vi sade vi skulle bevisa. □

Varför är det här ett intressant problem? Att rita grafer med så få korsningar som möjligt är inte bara ett estetiskt problem när man ritar saker på en blackboard, utan också ett praktiskt problem när man skall designa kretskort.

Kretskorten har nämligen många olika komponenter, som vi kan tänka oss som noder, som skall kopplas ihop med varandra. Så länge inte kopplingarna korsar varandra kan man helt enkelt måla dit dem, men om de skall korsa behöver man göra något mer komplicerat. Alltså är det av praktiskt intresse att hitta sätt att rita grafer som minimerar antalet korsningar – problemet i allmänhet med kretskortsdesign kallas för VLSI (Very Large Scale Integration).

Oberoende mängder i triangelfria grafer

Vi har redan innan visat resultat om antalet oberoende mängder i en graf – på en föreläsning visade vi Caro-Weis sats, och i en övning ger vi ett annat resultat om oberoende mängder med ett annat bevis.

Låt oss nu ge ytterligare ett resultat om oberoende mängder, denna gång under antagandet att grafen inte har några trianglar. Att detta borde hjälpa oss att hitta större oberoende mängder är någorlunda intuitivt – i en triangel kan vi ju bara ha med högst ett av de tre hörnen i vår oberoende mängd. Att inte innehålla någon triangel är dessutom en begränsning på antalet kanter grafen kan innehålla [11] – och desto färre kanter desto enklare blir det ju att hitta en oberoende mängd, eftersom varje kant ju säger att "du får bara ta en av dessa två noder till din oberoende mängd".

[10] Förutom om de utgår från samma nod – men vi kan aldrig tvingas att rita två kanter som utgår från samma nod så att de korsas. (Detta är ganska uppenbart men inte helt trivialt – fundera ett ögonblick på varför det är sant.)

[11] Detta är Turáns sats – en graf på n noder som inte innehåller några trianglar kan inte ha mer än $\frac{n^2}{4}$ kanter.

Detta maximala antal kanter uppnås för övrigt av att ta en graf som har två grupper A och B av $n/2$ noder var, och rita varje kant $\{a, b\}$ mellan A och B och inga kanter inuti varken A eller B.

En sådan graf kallas för *bipartit*, och har ju faktiskt en väldigt stor oberoende mängd.

Så resultatet vi ger säger oss något om hur stor oberoende mängd vi kan få om vi inte innehåller en triangel, och dessutom vet att varje nod har låg grad.

Teorem 10 (Ursprungligen av Ajtai-Komlós-Szemerédi, bevis av Shearer)**.** *Låt $G = (V, E)$ vara en triangelfri graf på n noder, och skriv $\Delta = \max_{v \in V} d_v$ för den maximala graden av en nod i G. Då finns det en oberoende mängd $S \subseteq V$ sådan att*

$$|S| \geq n \frac{\log_2(\Delta)}{8\Delta}.$$

Låt oss bryta ut den centrala idén i beviset av det här i ett lemma, bevisa det, och sedan använda lemmat för att bevisa satsen. I beviset kommer vi välja en slumpmässig oberoende mängd[12] S, och sedan visa en nedre begränsning av $\mathbb{E}[|S|]$. Som vanligt vill vi studera vårt problem "lokalt", runt en enda nod – så frågan vi vill ställa oss är: Om vi vet hur S ser ut överallt utom i v och dess grannar, vad kan vi säga om sannolikheten att $v \in S$? Och hur många av vs grannar ligger i genomsnitt i S?

Det visar sig att vi kan svara på dessa frågor, och ge exakta uttryck, men det kräver en del notation för att kunna göra det – formuleringen av lemmat blir nästan lika lång som beviset.

Lemma 11. *Låt $G = (V, E)$ vara en triangelfri graf på n noder, och låt S vara en likformigt slumpmässig oberoende mängd i G.*

Låt oss, för varje nod $v \in V$, skriva

$$H_v = G \setminus (v \cup N(v))$$

så att H_v alltså är hela G förutom just v och dess grannar.

Vi skriver $N_v(S)$ för mängden av grannar till en nod i $S \cap H_v$,[13] *alltså*

$$N(S) = \bigcup_{v \in S \cap H_v} N(v)$$

och vi låter $P_v = N(v) \setminus N(S)$ – så att P_v är mängden av grannar till v som hade kunnat läggas till till S.

Då gäller det för varje v att [14]

$$\mathbb{P}(v \in S \mid S \cap H_v) = \frac{1}{2^{|P_v|} + 1}.$$

och

$$\mathbb{E}[|N_v \cap S| \mid S \cap H_v] = \frac{|P_v|}{2 + 2^{1-|P_v|}}.$$

Bevis. Det är mycket notation i formuleringen av detta lemma, men beviset är faktiskt rätt så enkelt, i alla fall när man har rätt bild i huvudet av vad som pågår – att studera Figur 2 först för att förstå notationen innan man ger sig in i beviset är nog klokt.

[12] Vi väljer alltså varje oberoende mängd med samma sannolikhet – för det mesta brukar vi ju välja våra slumpvariabler som likformigt fördelade på en mängd vi förstår oss på väl, men det är så klart tillåtet att göra på detta viset också.

[13] Alltså mängden noder vi inte kan lägga till till $S \cap H_v$ utan att den slutar vara en oberoende mängd.

[14] Den uppmärksamma läsaren bör vara skeptisk mot vad vi just skrivit här, både i vänster och höger led.

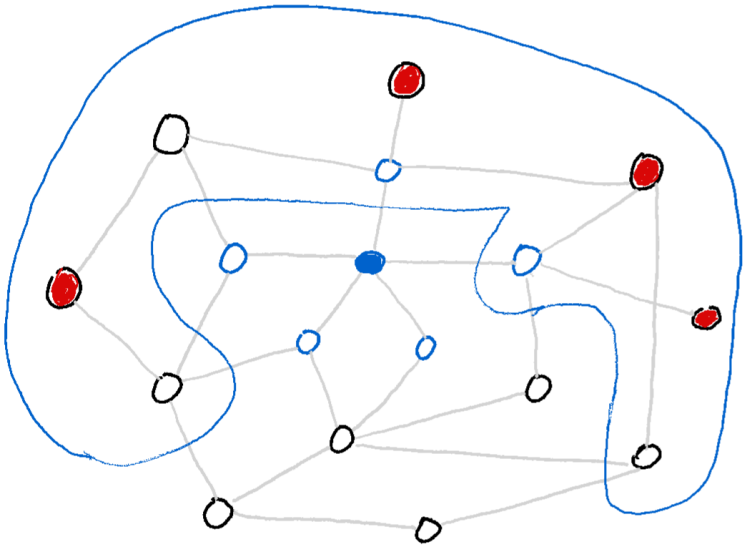
I vänster led skrev vi en betingad sannolikhet där vi betingade på en *slumpvariabel*, men vi har ju definierat betingade sannolikheter som att vi betingar på *händelser*.

I höger led påstår vi sedan att denna betingade sannolikhet blir lika med ett uttryck som inte är ett tal utan en *slumpvariabel* – S är ju slumpmässig, så varje uttryck som innehåller S kommer ju också vara slumpmässigt tills vi skriver ett $\mathbb{P}(\,)$ eller $\mathbb{E}[\,]$ för att omvandla det till ett tal.

Det finns definitioner som gör det här helt väldefinierat, men vi kan nöja oss med att betrakta detta som en läsligare notation för påståendet att, för varje oberoende mängd $W \subseteq H_v$, så är

$$\mathbb{P}(v \in S \mid S \cap H_v = W) = \left(2^{|P_v|} + 1\right)^{-1}.$$

I detta påstående, när vi valt ett W, blir ju $S \cap H_v = W$ en händelse, och höger led blir bara ett tal eftersom W är en fix mängd. Så detta är väldefinierat enligt våra definitioner.



Figur 2: En triangelfri graf, med noden v ifylld blå, noderna i $N(v)$ ihåligt blå, noder i H_v svarta, noder i $S \cap H_v$ ifyllda i rött, och mängden $N_v(S)$ inringad med en blå cirkel.

Vad vi behöver svara på är följande fråga: Givet att vi vet vilka noder i H_v som är med i S, hur många olika sätt kan vi utvidga S till hela G, alltså inklusive $v \cup N(v)$, och hur många av dessa sätt har $v \in S$?

Den senare delen av frågan är enkel att besvara – så snart vi lagt in v i S så får så klart inga av dess grannar vara med i S, så det finns exakt ett sätt att utvidga S från H_v till hela G sådant att $v \in S$.

Hur många sätt finns det att utvidga S om vi säger att $v \notin S$? Jo, för varje granne till v ligger den antingen i $N_v(S)$, och får inte läggas till, eller så ligger grannen i $N_v(S)^c$ och vi får lov att lägga till den.

Eftersom grafen inte innehåller några trianglar finns det inga kanter mellan några två noder i $N(v)$ – alltså kan våra val av noder ur $N(v) \cap N_v(S)^c$ att lägga till till S inte blockera varandra, så varje delmängd till $N(v) \cap N_v(S)^c$ är ett giltigt val.

Alltså finns det $2^{|N(v) \cap N_v(S)^c|}$ sätt att utvidga S till hela G sådana att $v \notin S$.

Eftersom S var likformigt fördelad på mängden av oberoende mängder måste varje av dessa alternativ vara lika sannolikt, och alltså är sannolikheten att vi väljer det enda alternativet där $v \in S$ precis

$$\frac{1}{2^{|N(v) \cap N_v(S)^c|} + 1}$$

såsom vi önskade bevisa.

För att räkna ut väntevärdet av antalet noder i $N(v)$ som ligger i S kan vi räkna likadant. Först noterar vi att $N(v) \cap S = P_v \cap S$ – en nod som inte ligger i P_v har redan en granne i S, så den kan omöjligen hamna i S.

Vi har sett att det finns totalt $2^{|P_v|} + 1$ möjliga värden för $P_v \cap S$, och

alla är lika sannolika, så

$$\begin{aligned}
\mathbb{E}\left[|N(v) \cap S| \mid S \cap H_v\right] &= \mathbb{E}\left[|P_v \cap S| \mid S \cap H_v\right] \\
&= 0 \cdot \mathbb{P}\left(v \in S \mid S \cap H_v\right) \\
&\quad + \sum_{Q \subseteq P_v} |Q| \mathbb{P}\left(P_v \cap S = Q \mid S \cap H_v\right) \\
&= \sum_{i=0}^{|P_v|} \sum_{\substack{Q \subseteq P_v \\ |Q|=i}} \frac{i}{2^{|P_v|}+1} \\
&= \frac{1}{2^{|P_v|}+1} \sum_{i=0}^{|P_v|} i \binom{|P_v|}{i} \\
&= \frac{|P_v|\, 2^{|P_v|-1}}{2^{|P_v|}+1} = \frac{|P_v|}{2^{1-|P_v|}+2}
\end{aligned}$$

vilket är precis vad vi ville bevisa.[15] □

[15] För att ta oss från näst sista raden till sista raden använde vi oss av likheten

$$\sum_{k=0}^{n} k \binom{n}{k} = n 2^{n-1}.$$

Att bevisa denna likhet med ett kombinatoriskt bevis är en av våra extraövningar.

Med detta resultat i handen kan vi nu ge vårt bevis för Teorem 10.

Bevis av Teorem 10. Om $\Delta < 16$ följer resultatet av Caro-Weis sats, så vi antar att $\Delta \geq 16$. Låt S vara en likformigt slumpmässig oberoende mängd i G.

Vi definierar, för varje $v \in V$, en slumpvariabel X_v som

$$X_v = \Delta \mathbb{1}_{\{v \in S\}} + |N(v) \cap S|.$$

Låt oss nu studera väntevärdet av summan av dessa X_v. Vi ser att det är sant, för alla utfall, att

$$\begin{aligned}
\sum_{v \in V} X_v &= \sum_{v \in V} \Delta \mathbb{1}_{\{v \in S\}} + |N(v) \cap S| \\
&= \Delta |S| + \sum_{v \in V} |N(v) \cap S| \\
&= \Delta |S| + \sum_{w \in S} |N(w)|.
\end{aligned}$$

Vad hände i det sista steget? Jo, vi observerar att de två summorna bara är olika sätt att räkna samma sak – antalet kanter mellan en nod i S och en utanför S. I den första summan summerar vi över alla noder, och räknar antalet kanter från den noden till en nod i S, och i den andra summan summerar vi över alla noder i S och räknar antalet kanter från den till någonting utanför S.

Vi vet också att alla noder har grad högst Δ, så att $|N(w)| \leq \Delta$ för alla w. Alltså måste vi ha från vår räkning att

$$\sum_{v \in V} X_v = \Delta |S| + \sum_{w \in S} |N(w)| \leq \Delta |S| + \sum_{w \in S} \Delta = 2\Delta |S|.$$

Så om vi kan hitta en nedre begränsing på $\sum_{v \in V} X_v$ kommer vi alltså att ha en nedre begränsning på $|S|$, vilket ju är vad vi är ute efter.

Så låt oss studera $\mathbb{E}[X_v]$. Vi kan använda vårt lemma och lagen om total sannolikhet [16] för att få ut att

$$\begin{aligned}\mathbb{E}[X_v] &= \mathbb{E}[\mathbb{E}[X_v \mid S \cap H_v]] \\ &= \mathbb{E}\left[\mathbb{E}\left[\Delta \mathbb{1}_{\{v \in S\}} + |N_v \cap S| \;\middle|\; S \cap H_v\right]\right] \\ &= \mathbb{E}\left[\Delta \mathbb{P}(v \in S \mid S \cap H_v) + \frac{|P_v|}{2^{1-|P_v|}+2}\right] \\ &= \mathbb{E}\left[\frac{\Delta}{2^{|P_v|}+1} + \frac{|P_v|}{2^{1-|P_v|}+2}\right]\end{aligned}$$

Vad vi vill göra nu är att bevisa att uttrycket inuti väntevärdet är större än $\frac{1}{4}\log_2(\Delta)$ för *alla* utfall. Antag alltså för motsägelse att det är *mindre* än detta. Detta antagande ger oss omedelbart att $|P_v| > 0$, eftersom om $|P_v| = 0$ blir uttrycket helt enkelt $\frac{1}{2}\Delta$, och det är definitivt större än $\frac{1}{4}\log_2(\Delta)$ när $\Delta \geq 16$, vilket vi har antagit.

Vi kan sedan räkna att[17]

$$\begin{gathered}\frac{\Delta}{2^{|P_v|}+1} + \frac{|P_v|}{2^{1-|P_v|}+2} < \frac{\log_2(\Delta)}{4} \\ \Updownarrow \\ 2^{|P_v|}(\log_2(\Delta) - 2|P_v|) > 4\Delta - \log_2(\Delta).\end{gathered}$$

Höger led av detta är positivt, så alltså kan inte parentesen i vänster led vara negativ, så $\log_2(\Delta) > 2|P_v|$. Alltså kan vi räkna

$$\log_2(\Delta) > 2|P_v| \Leftrightarrow 2^{\frac{1}{2}\log_2(\Delta)} > 2^{|P_v|} \Leftrightarrow \sqrt{\Delta} > 2^{|P_v|}$$

så

$$4\Delta - \log_2(\Delta) < 2^{|P_v|}(\log_2(\Delta) - 2|P_v|) < \sqrt{\Delta}(\log_2(\Delta) - 2)$$

och detta är till slut en olikhet som enbart involverar Δ! Så vi kan helt enkelt studera funktionen

$$\sqrt{\Delta}(\log_2(\Delta) - 2) - 4\Delta - \log_2(\Delta)$$

och konstatera att denna är negativ för alla $\Delta \geq 16$, så olikheten måste vara falsk, och alltså följer det att

$$\frac{\Delta}{2^{|P_v|}+1} + \frac{|P_v|}{2^{1-|P_v|}+2} \geq \frac{\log_2(\Delta)}{4}$$

oavsett vad P_v är.

Så

$$\mathbb{E}[X_v] = \mathbb{E}\left[\frac{\Delta}{2^{|P_v|}+1} + \frac{|P_v|}{2^{1-|P_v|}+2}\right] \geq \mathbb{E}\left[\frac{\log_2(\Delta)}{4}\right] = \frac{\log_2(\Delta)}{4}$$

och alltså är

$$\mathbb{E}\left[\sum_{v \in V} X_v\right] \geq \frac{n\log_2(\Delta)}{4}$$

[16] Här ser vi en av de stora anledningarna till att använda våra betingningar på slumpvariabler istället för på händelser. Hade vi betingat på händelsen att $S \cap H_v = W$ för olika W hade vi behövt skriva

$$\mathbb{E}[X_v] = \sum_{\substack{W \\ \text{ober. mgd. i } H_v}} \mathbb{E}[X_v \mid S \cap H_v = W] \cdot \mathbb{P}(S \cap H_v = W),$$

vilket ju är ett uttryck så stort att vi knappt kan formatera det i marginalen!

Med vårt alternativa skrivsätt kan vi formulera lagen om total sannolikhet som att den säger att

$$\mathbb{E}[A] = \mathbb{E}[\mathbb{E}[A \mid B]]$$

för varje par av slumpvariabler A och B – en mycket renare formulering, som ger kortare formler.

[17] Att gå från första till andra olikheten här kräver så klart ett antal steg – vi skippar att faktiskt inkludera dem, eftersom de inte är så intressanta, men känn dig inte dum om du inte omedelbart ser varför dessa olikheter är ekvivalenta, det gör nog ingen.

och enligt vår tidigare räkning har vi också

$$2\Delta|S| \geq \sum_{v \in V} X_v$$

så vad vi sett är att

$$\mathbb{E}\left[2\Delta|S|\right] \geq \frac{n \log_2(\Delta)}{4}$$

vilket ger satsen, enligt vårt vanliga resonemang om att väntevärdet inte kan vara mindre än varje givet utfall. □

Längsta ökande delföljden i en permutation

Övningar

Övning 1. Vi introducerade, i en övning till föreläsning 9, konceptet med *turneringar*. En turnering med n lag är ett sätt att rikta K_n – det är alltså en riktad graf med en kant mellan varje par av noder, där kanten kan peka åt endera hållet. Vi tänker oss det som att alla lag spelar mot alla andra lag, och kanterna pekar från vinnare till förlorare.

Bevisa att det finns en turnering med n lag som innehåller åtminstone $n!2^{-n}$ Hamiltoncykler.[18]

[18] Med Hamiltoncykel i en riktad graf menar vi att vi alltid går i den riktning kanterna pekar – vi får aldrig lov att gå baklänges längst en kant.