Föreläsning 1: Permutationer och kombinationer · 1MA020

Vilhelm Agdur[1]

16 januari 2023

[1] Plus redigeringar och lösningsförslag av studenter, se `contributors.md`.
`vilhelm.agdur@math.uu.se`

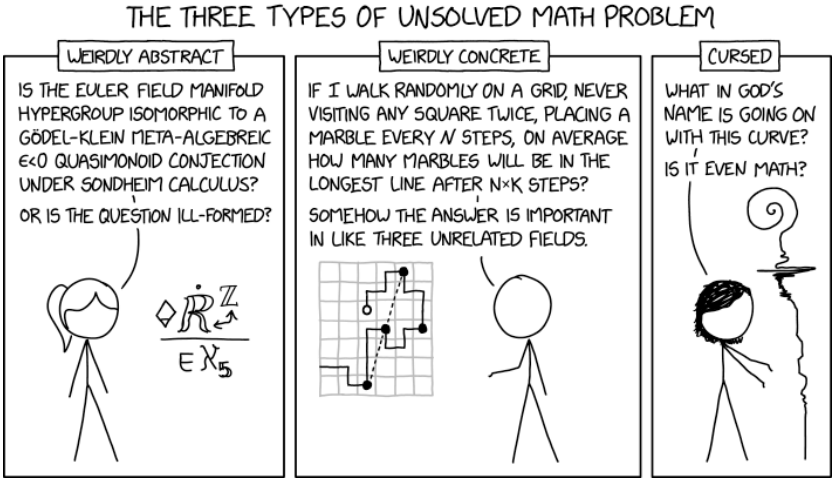
Vi börjar med att fråga oss vad kombinatorik ens är för något. Sedan introducerar vi några väldigt grundläggande begrepp och principer i ämnet, och tillämpar dem på att diskutera permutationer och kombinationer.

Vad är kombinatorik?

Jag hörde en gång, på en fest under min masterutbildning, en utläggning av en doktorand om att all matematik handlar om att reducera sina problem till en enklare form – och i slutändan var alla matematikproblem antingen linjär algebra, i vilket fall de var lätta, eller så var de kombinatorik, i vilket fall de var svåra. Vi skall alltså studera den svåra delen av matematiken.

En annan överförenklande kategorisering av matematiken ges oss av Randall Munroe.[2] Kombinatorik sysslar med den mellersta sortens problem – där det är lätt att förstå frågan, och inga märkliga kontinuerliga objekt är involverade, men svaret ändå kan vara komplicerat att ta reda på.

[2] Randall Munroe. Unsolved math problems. `https://xkcd.com/2529/`



En mer ordboksmässig definition av vad kombinatorik är vore att säga att det handlar om att räkna saker, när sakerna är ändligt många och diskreta. Detta är dock heller ingen precis eller uttömmande definition, så det finns saker som är kombinatorik utan att nödvändigtvis handla om att räkna saker, till exempel inom grafteori.

Varför studera kombinatorik?

Kombinatorik har som redan nämnts tillämpningar i ren matematik – många problem inom andra grenar av matematiken kan reduceras till problem i kombinatorik. Det har också otaliga tillämpningar utanför den rena matematiken:

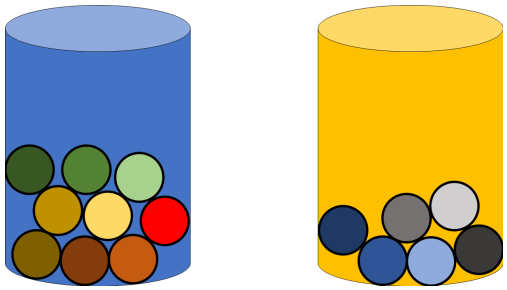
1. Nätverk och grafer
2. Analys av algoritmer
3. Design av kretskort
4. Design av experiment

Merparten av alla pussel-spel av typen sudoku, eller "flytta bilarna för att få ut en specifik bil", etc., kan ses som rena kombinatorikproblem.

Additions- och multiplikations-reglerna

Definition 1 (Additions-regeln)**.** Om A är en mängd av n objekt och B är en mängd av m objekt så finns det $n+m$ sätt att välja ett objekt från A *eller* ett objekt från B. Eller formulerat i symboler, om $|A| = n$ och $|B| = m$ så är $|A \coprod B| = n + m$. [3]

Exempel 2. Vi har två burkar med olikfärgade kulor, såsom i figur 1. Om vi ska plocka ut en kula från en av burkarna, på hur många sätt kan vi göra det?



Figur 1: Två separata burkar med kulor i, där den vänstra har nio kulor och den högra sex.

Vi kan använda additionsregeln för att beräkna att det finns $9+6 = 15$, sätt att välja en kula, vilket är samma som totala antalet kulor.

Exempel 3. En restaurang har en meny med fyra drinkar, fem förrätter, tio huvudrätter, och tre desserter. Hur många saker har de på menyn?

Additions-regeln säger oss att svaret är $4+5+10+3 = 22$.

Definition 4 (Multiplikations-regeln)**.** Om A är en mängd av n objekt och B är en mängd av m objekt så finns det nm sätt att välja ett objekt

[3] Symbolen $\coprod$ (Man ser ibland istället notationen $\uplus$ för detta) betyder *disjunkt union* – vi tar unionen av de två mängderna, men vi tvingar mängderna att vara disjunkta genom att komma ihåg vilken mängd varje element kom från. Så om A och B inte har några gemensamma element är det samma sak som $\cup$, men om de har gemensamma element gäller att t.ex.

$$\{1,2,3\} \cup \{3,4\} = \{1,2,3,4\},$$

emedan

$$\{1,2,3\} \coprod \{3,4\} = \{(1,A),(2,A),(3,A),(3,B),(4,B)\},$$

så de har alltså olika antal medlemmar.

För det allra mesta behöver man inte vara så här rigorös, men det kan vara bra att ha i bakhuvudet att summaregeln inte räknar antalet element i $A \cup B$ om A och B kan tänkas ha gemensamma element. Vad vi gör i det fallet kommer vi återkomma till senare, när vi diskuterar inklusion-exklusion.

från A *och* ett objekt från B. Eller ekvivalent, det finns nm sätt att välja ett par av ett objekt ur A och ett objekt ur B. Eller uttryckt i symboler

$$|A \times B| = |\{(a, b) \mid a \in A, b \in B\}| = nm.$$

Exempel 5. Om vi har samma två burkar som i Exempel 2, på hur många sätt kan man välja en kula från den blå burken och en kula från den gula burken?

Antalet olika sätt att välja två kulor, en från ena burken och en från den andra, ges enligt multiplikationsregeln av produkten av antalet bollar i varje burk, alltså $9 \cdot 6 = 54$.

Exempel 6. Om du besöker restaurangen i Exempel 3, hur många olika sätt finns det att beställa en trerätters middag med en drink till? [4] Multiplikations-regeln säger oss att svaret är $4 \cdot 5 \cdot 10 \cdot 3 = 600$.

[4] En fullständigt teoretisk fråga, eftersom ingen faktiskt har råd med det i dagens ekonomi.

Strängar

Definition 7. En *sträng* s (eller ett *ord*) av längd n på en mängd X (kallad *alfabetet* för strängen) är en funktion

$$s : \{1, 2, \ldots, n\} = [n] \to X$$

där s_i är den $i$te bokstaven i ordet.[5] Vi skriver detta oftast som $s = x_1 x_2 \ldots x_n$, där $x_i = s(i)$.

[5] Från och med nu kommer vi konsekvent använda notationen $[n]$ för mängden av tal mellan 1 och n.

Exempel 8 (Binära strängar)**.** Låt $X = \{0, 1\}$. Strängar $s : [n] \to X$ kallas för *binära strängar*. Det finns 2^n strängar av längd n.[6]

Hur vet vi detta? Det finns två val för varje bokstav, så multiplikationsregeln säger oss att det måste finnas $2 \cdot 2 \cdot \ldots \cdot 2 = 2^n$ att göra ett val av vad varje bokstav skall vara.

[6] Så det finns till exempel åtta binära strängar av längd tre, nämligen

$$000, 001, 010, 011, 100, 101, 110, 111.$$

Exempel 9 (m-ära strängar)**.** Låt $X = \{0, 1, \ldots, m-1\}$. Strängar med detta alfabetet kallas för m-ära strängar. Om $m = 2$ är de binära, om $m = 3$ är de ternära.

Precis som för de binära strängarna kan vi använda multiplikationsregeln för att räkna ut hur många m-ära strängar det finns av längd n. För varje position i ordet har vi m olika val av bokstav – en per bokstav i vårt alfabete – och vi skall välja n gånger. Alltså ger multiplikationsregeln att det finns totalt m^n m-ära strängar av längd n.

För generella X kallar vi en sträng $s : [n] \to X$ för en X-sträng.

Permutationer

Definition 10. En sträng $s : [k] \to X$ kallas för en *permutation* av längd k av elementen i X om alla bokstäverna i s är olika, det vill säga om $s(i) \neq s(j)$ ifall $i \neq j$.

Självklart måste $|X| \geq k$ för att det skall existera några permutationer av längd k av X.[7]

[7] Hur hade du bevisat det?

Exempel 11. Låt $X = [3]$. Det finns 6 permutationer av längd 2 av X[8] – vi kan se detta med hjälp av multiplikationsprincipen: Vi har tre val av första bokstav, men när vi valt den första bokstaven har vi bara två val kvar av andra bokstav, eftersom vi inte får ha två av samma. Alltså är det totala antalet $3 \cdot 2 = 6$.

[8] Dessa är, specifikt,

$$12, 13, 21, 23, 31, 32.$$

Definition 12. För $n = 1, 2, \ldots$, definiera $n! = n(n-1)\ldots 2 \cdot 1$. Definiera $0! = 1$.[9]

För $k \leq n$, definiera $P(n,k) = \frac{n!}{(n-k)!}$. Lägg märke till att $P(n,n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$.

[9] Att vi låter 0! vara lika med ett är för att vi ser det som produkten av inga tal alls, vilket är bekvämt att se som att det blir 1. Varför detta är så kommer vi kanske att återkomma till när vi pratar om rekursioner.

Proposition 13. *Om $|X| = n$ och $0 \leq k \leq n$ så finns det $P(n,k)$ permutationer av längd k från X.*

Bevis. Vi bevisar detta med hjälp av multiplikationsprincipen – så vi skall räkna hur många sätt vi kan välja vår permutation $x_1 x_2 \ldots x_k$ på. Det finns så klart $|X| = n$ sätt att välja första bokstaven x_1 i vår permutation. När vi sedan skall välja x_2 får den inte vara lika med x_1, så vi väljer ett element ur $X \setminus \{x_1\}$, och $|X \setminus \{x_1\}| = n - 1$. Likaledes för x_3 så får den varken vara lika med x_1 eller x_2, så vi väljer från $X \setminus \{x_1, x_2\}$, och har $n - 2$ val.

Den här processen fortsätter tills vi skall välja x_k, och i det skedet har vi tagit bort $k - 1$ val, och har alltså $|X \setminus \{x_1, x_2, \ldots, x_{k-1}\}| = n - (k-1)$ bokstäver kvar att välja på.

Multiplikationsregeln säger oss att det totala antalet permutationer är lika med produkten av antalet val vi hade i varje steg, det vill säga

$$\begin{aligned} n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-(k-1)) &= \frac{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1}{(n-k) \cdot \ldots \cdot 2 \cdot 1} \\ &= \frac{n!}{(n-k)!} = P(n,k). \end{aligned}$$

□

Exempel 14. På hur många olika sätt kan n personer sitta runt ett runt bord?[10]

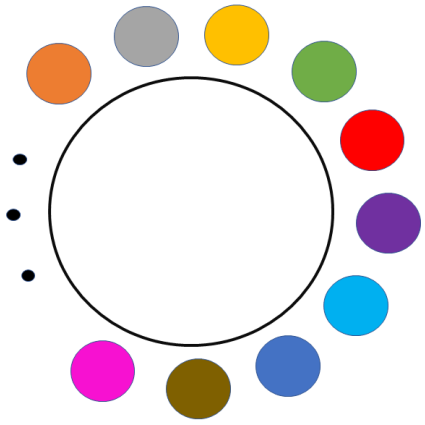
Det finns två olika sätt vi kan se på frågan[11] – antingen är det skillnad på de olika stolarna runt bordet (vissa kan se ut genom fönstret, andra inte), så att vi får olika sätt att placera folk runt bordet genom att rotera hela placeringen, eller så är det enda som spelar roll ordningen de sitter i, och vi ser olika rotationer av samma ordning som samma sätt att sitta runt bordet.

Om platserna har etiketter, så att det inte bara är ordningen som spelar roll, så kan vi numrera platserna från plats 1 till plats n. Om vi

[10] Det finns en liten ritning av detta i anteckningarna från föregående år, och jag lär rita den på den faktiska föreläsningen.

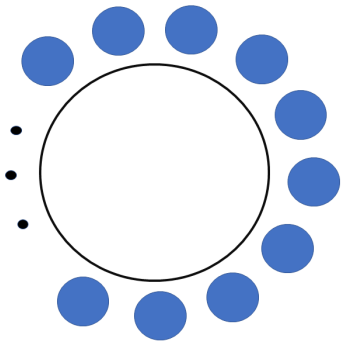
[11] Detta är ett exempel av skillnaden mellan problem med etiketter och utan, vilket är ett generellt fenomen som kommer återkomma gång på gång. Här är det platserna runt bordet som kan ha etiketter eller inte. Var noggrann med att fundera kring vilken typ av

kallar mängden med gäster för X blir alltså varje placering ett X-ord – vi kan skriva den som "gäst ett, gäst två, etc.". Och eftersom varje person bara kan sitta på en stol blir detta alltså en permutation – och vi vet att det finns $n!$ permutationer av längd n ur ett alfabete med n bokstäver.



Figur 2: Ett bord med olikfärgade stolar, så att vi kan se skillnad på stolarna – det är skillnad mellan att sitta på en blå pall och i en orange fåtölj. Färgerna är alltså etiketter på platserna.

Om platserna är oetiketterade, det vill säga att det enda vi bryr oss om är ordningen folk sitter i, får vi räkna på ett annat sätt. Givet en placering kan vi godtyckligt välja en person som "först", och sedan numrera platserna i medurs ordning. För varje av de n sätten att välja vem som är först får vi alltså en placering där platserna har etiketter.



Figur 3: Ett bord med identiska stolar runt bordet. Här är alltså varje plats likadan och det kommer endast spela roll vem man sitter bredvid, till skillnad från vid förra bordet.

Om alla som sitter vid bordet flyttar ett steg åt höger kommer vi få precis samma bordsplacering igen, eftersom vi inte kan se skillnad på stolarna och alla fortfarande sitter bredvid samma personer.

Detta ger oss ett annat sätt att räkna antalet placeringar med etiketter – vi räknar antalet utan etiketter, kallar det m, och får alltså att antalet med etiketter är nm.

Men eftersom vi redan vet att antalet när platserna har etiketter är

$n!$ så får vi alltså av detta att $n! = nm$, eller $m = \frac{n!}{n} = (n-1)!$, och vi har räknat antalet utan etiketter till $(n-1)!$.[12]

[12] Detta är ett vanligt sätt att resonera inom kombinatorik – vi hittade två olika sätt att räkna samma sak, och fick på så sätt ut en likhet ($nm = n!$) som vi kunde använda för att räkna en annan sak.

Kombinationer

Definition 15. För en mängd X så är en *kombination* av element ur X en delmängd $A \subseteq X$.[13]

[13] Vi talade innan om etiketter och inte. Man kan se en kombination som en permutation utan etiketter – vi vet bara vilka element som är med, inte i vilken ordning de kommer.

Exempel 16. Det finns 6 kombinationer av storlek 2 från $X = \{a, b, c, d\}$, nämligen

$$\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}.$$

Definition 17. För $0 \leq k \leq n$, låt $\binom{n}{k} = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k)!}$. Man ser också notationerna $C(n, k)$, nCk, eller C_k^n för detta, men vi håller oss till $\binom{n}{k}$.

Proposition 18. *Om $|X| = n$ och $0 \leq k \leq n$ så finns det $\binom{n}{k}$ kombinationer av storlek k från X.*

Bevis. Även detta bevisar vi med "räkna på två olika sätt"-metoden. Låt oss börja med att räkna antalet *permutationer* igen, på ett annat sätt än vi gjorde i beviset av Proposition 13.

Istället för att tänka oss att vi väljer en bokstav i taget, kan vi tänka oss att vi först väljer en mängd A av bokstaver som skall vara med – och då måste ju $|A| = k$ eftersom varje bokstav skall dyka upp exakt en gång – och sedan väljer en ordning i vilken bokstäverna skall dyka upp.

Antalet sätt att välja en ordning för våra k bokstäver är precis antalet permutationer av längd k från alfabetet A, vilket vi vet är $P(k, k)$. Så om vi betecknar antalet sätt att välja mängden A med m, så säger oss multiplikationsregeln att antalet permutationer av längd k från X måste vara $m \cdot P(k, k)$.

Men vi vet ju också, från hur vi räknade antalet permutationer innan, att $P(n, k) = \frac{n!}{(n-k)!}$ och $P(k, k) = k!$. Så vad vi har visat är att

$$\frac{n!}{(n-k)!} = P(n, k) = mP(k, k) = mk!$$

eller, om vi löser för m, att

$$m = \frac{n!}{k!(n-k)!}$$

vilket är vad vi ville bevisa. □

Proposition 19. *För alla $n \geq 0$ och alla $0 \leq k \leq n$ gäller det att*

$$\binom{n}{k} = \binom{n}{n-k}.$$

Vi ger två olika bevis av denna proposition. Det första är algebraiskt:

Bevis.

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k!(n-k)!} \\ &= \frac{n!}{(n-(n-k))!(n-k)!} \\ &= \frac{n!}{(n-k)!(n-(n-k))!} = \binom{n}{n-k}.\end{aligned}$$

□

Det andra är kombinatoriskt:[14]

Bevis. Låt X vara en mängd med n element. $\binom{n}{k}$ räknar antalet sätt att välja en delmängd $A \subseteq X$ av storlek k. Men varje sådan delmängd A har ett komplement $X \setminus A$ av storlek $n-k$, och för varje delmängd av storlek $n-k$ kan vi få en av storlek k genom att ta dess komplement.

Delmängder av storlek k och delmängder av storlek $n-k$ står alltså i ett-till-ett-korrespondens med varandra, det finns en bijektion mellan dem, så det måste finnas lika många av storlek k som av storlek $n-k$.

Men vi vet att antalet delmängder av storlek $n-$ är $\binom{n}{n-k}$, och alltså måste $\binom{n}{k} = \binom{n}{n-k}$.

□

[14] Vad menar vi när vi säger att det här beviset är "kombinatoriskt", till skillnad från det andra beviset? Nyckeln är att vi här visade att de två mängderna – mängden av delmängder av storlek k och mängden av delmängder av storlek $n-k$ – har lika många medlemmar genom att uppvisa en bijektion mellan dem, emedan vi i det algebraiska beviset bara manipulerade våra formler för att visa att de var lika.

Bijektionen vi hittade här är själv ett *kombinatoriskt* objekt, och det berättar mer för oss än bara att mängderna har lika många medlemmar. Man kan se det som att den är en *anledning* till varför de har lika många mängder.

Denna bevismetod, att hitta en bijektion, kommer vara ett återkommande tema – och likaså att bijektionerna ger oss mer förståelse för objekten vi studerar än vad ett algebraiskt bevis gör.

Övningar

Övning 1. Tjugofyra studenter ska sitta vid ett långt bord[15] och skriva en tenta. Tio av dem är väldigt benägna att fuska genom att kolla på sin kompis tenta.

Deras kombinatoriklärare bestämmer att dessa tio studenter måste sitta på platser med udda nummer, så att de inte kan hamna bredvid varandra och fuska.

Hur många sätt finns det att placera studenterna vid bordet?

[15] Ni slipper alltså runda bord i denna övningen! Bordet har en första plats, en andra plats, och så vidare till tjugofjärde platsen.

Övning 2. Ge ett algebraiskt bevis för att

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

Övning 3. Ge ett kombinatoriskt bevis för att[16]

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

[16] Ledtråd: Tänk på att välja grupper med ledare för ett projekt.

Övning 4. Ge ett kombinatoriskt bevis för att

$$\binom{n}{2}\binom{n-2}{k-2} = \binom{n}{k}\binom{k}{2}.$$

Övning 5. Antag att du har två mängder A och B, med $|A| = 15$ och $|B| = 7$.

1. Hur många sätt finns det att välja ett objekt från A eller ett från B?
2. Hur många sätt finns det att välja ett objekt från A och ett från B?
3. Vad är $|A \times B|$?
4. Vad är $|A \coprod B|$?
5. Vad är det största och minsta värde som $A \cup B$ kan ta?
6. Vad är det största och minsta värde som $A \cap B$ kan ta?

Övning 6. Du har sökt ett prestigefyllt internship, och ska klä dig för intervjun. Du inser att du borde ha slips på dig, och ser att du äger fem seriösa slipsar och sju slipsar med komiska tryck.

a) Hur många sätt kan du välja slips för intervjun på?

Efter lite eftertanke kommer du ihåg att jobbet du sökt är som clown,[17,18] så du borde nog ha på dig två slipsar på samma gång, eftersom det är väldigt komiskt.

b) På hur många sätt kan du välja två slipsar att ha på dig på samma gång? **c)** Hur många sätt kan du välja en seriös slips och en med ett komiskt tryck på?

[17] Och tyvärr äger du ingen sådan där skoj fluga som kan spruta vatten i ansiktet på folk.

[18] Denna övningen är stulen från internet, och den handlade om en clownjobbintervju redan från början. Jag valde den helt baserat på hur mycket jag skrattade åt hur de antydde att deras studenter var clowner.

Lösningsförslag till övningar

Lösning 1. Vi börjar med att rita upp en bild för situationen.

Figur 4: Ett långt bord med 24 numrerade stolar.

Enligt uppgiften behöver vi placera ut de fuskande eleverna på udda stolsplatser, alltså ska vi placera ut 10 elever på 12 platser. Detta kan göras på $P(12, 10)$ sätt.

Därefter har vi 14 elever kvar att placeras ut på de kvarvarande 14 platserna. Det kan göras på $P(14, 14)$ sätt.

Det totala antalet sättet att placera ut alla elever blir därmed

$$P(12, 10)P(14, 14) = \frac{12!14!}{2!}.$$

Anledningen till att vi använder permutationer i lösningen är för att vi ser både stolsplatserna och studenterna som särskiljbara.

Tips. Viktigt i liknande uppgifter är att identifiera ifall platserna, stolarna i det här fallet, är särskiljbara eller inte. Om de är särskiljbara, som i det här fallet, så använder vi oss av permutationer. Är de inte unika så får vi använda oss av kombinationer istället. I vår figur numrerar vi alltså stolsplatserna, så att vi kan se skillnad på dem på vilket nummer de har.

Ett sätt att enklare förstå uppgiften är att vi ska dela ut stolsnummer till eleverna, istället för att placera ut eleverna på stolarna. Då kan det bli enklare att förstå varför det går att placera ut de 10 fuskande eleverna på de 12 udda platserna på $P(12, 10)$ olika sätt – 12 stolsnummer ska delas ut till 10 personer.

Lösning 2.

$$\begin{aligned} n\binom{n-1}{k-1} &= \frac{n(n-1)!}{(k-1)!(n-1-(k-1))!} \\ &= \frac{n(n-1)!}{(k-1)!(n-k)!} \\ &= \frac{kn!}{k!(n-k)!} = k\binom{n}{k} \end{aligned}$$

Tips. Expandera utrycket genom att använda definitionen av binomialkoefficienter

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Tänk på att n-fakultet kan skrivas som

$$n! = n(n-1)(n-2)...2 \cdot 1$$

och att

$$\frac{n}{n!} = \frac{1}{(n-1)!} \qquad \text{och} \qquad n(n-1)! = n!.$$

Lösning 3. Från sidnoten får vi tipset att tänka på det som att välja en grupp med ledare. Vi försöker nu studera vänsterledet för sig och högerledet för sig för att kombinatoriskt bevisa likheten.

Vi kollar på vänsterledet först: Vi vill välja en grupp med k personer i och vi har totalt n stycken personer att välja på. Antalet sätt vi kan skapa denna gruppen på ges av $\binom{n}{k}$. Vi har alltså beräknat antalet sätt att skapa en grupp med k personer.

Nu vill vi välja en ledare bland dessa personer. Vi har k potentiella ledare, så multiplikationsregeln säger oss att vi får antalet sätt att välja en grupp med ledare genom att multiplicera antalet sätt att välja en grupp med antalet sätt att välja en ledare, alltså

$$k\binom{n}{k}.$$

Nu tittar vi på högerledet: Vi vill visa att högerledet också beräknar antalet sätt att skapa en grupp med k personer varav en person är ledare. Vi har n personer att välja på och vi ska ha en grupp på k personer, varav en ska vara ledare.

Vi börjar med att välja en person som ska vara vår ledare, vilket vi kan göra på n sätt. Sedan vill vi välja en grupp till den här ledaren. Vi har $n-1$ personer kvar att välja på och $k-1$ platser kvar att fylla upp i gruppen. Antalet sätt att skapa gruppen av resterande personer blir då

$$\binom{n-1}{k-1}.$$

Så antalet sätt att skapa en grupp med en ledare och $k-1$ medlemmar (alltså totalt k medlemmar) är

$$n\binom{n-1}{k-1}.$$

Tips. 1. I denna uppgiften använde vi oss av att vi ska skapa grupper. Ett bra sätt att lösa liknande uppgifter är att se det som att vi ska skapa grupper med personer av olika slag. Det kan vara en grupp med en eller flera ledare, grupper av olika storlekar med olika många personer som ska väljas ut eller plockas bort med mera. Försök att skapa ett sammanhang.

2. Är det svårt att hitta ett sammanhang så försök att identifiera variablerna en efter en, så i detta fallet försök först att identifiera vad k

skulle kunna innebära och vad $\binom{n}{k}$ skulle kunna innebära. Försök också att starta med en sida, så antingen vänster led eller höger led. Identifiera de olika variablerna (till exempel i ett sammanhang) på den sidan och försök sedan skapa en matchning med andra sidan.

3. Ett sätt att se på det är som ett händelseförlopp. Betrakta vänster led i Övning 4: Först händer en sak – vi väljer två av totalt n stycken saker. Sedan, efter att vi gjort det "sker" andra parentesen som säger att vi nu väljer $k-2$ saker av en hög som nu är 2 färre än den var förut. Genom detta kan vi försöka skapa oss en bild av ett händelseförlopp som dessa uttryck representerar.

Lösning 4. Här kan vi tänka på ungefär samma sätt som uppgift 3, men nu är skillnaden att vi ska välja 2 ledare istället för en.

Vi har en grupp på n personer och vi vill välja ut en liten grupp med k personer i varav 2 kommer utses till ledare.

Vi börjar med vänsterledet: Vi har alltså n personer och vi vill välja två stycken ledare av alla de n personerna. Detta kan vi göra på

$$\binom{n}{2}$$

sätt.

När det är gjort så har vi $n-2$ personer kvar som inte blivit valda, och av de $n-2$ personerna vill vi välja ut $k-2$ stycken för att skapa en grupp som tillsammans med de två ledarna skapar en grupp på k personer.

Gruppen på $k-2$ personer kan vi skapa på $\binom{n-2}{k-2}$ sätt, eftersom vi har $n-2$ personer kvar att välja bland. När vi då multiplicerar

$$\binom{n}{2}\binom{n-2}{k-2}$$

får vi alltså antalet sätt att forma en grupp med k personer varav 2 stycken är ledare.

Vi kollar på högerledet: I högerledet tänker vi först att vi vill skapa en grupp med k personer av de n stycken möjliga personerna. Antalet sätt att göra detta på är $\binom{n}{k}$. När vi har skapat en grupp med k personer i så vill vi välja två stycken ledare. Detta kan vi göra på

$$\binom{k}{2}$$

sätt eftersom vi har k stycken möjliga ledare.

Poängen är alltså att HL och VL bara gör saker i olika ordning. VL väljer ledarna först och gruppen sedan medans HL väljer gruppen först och sedan väljer ledarna i gruppen. Nu har vi visat att både vänsterledet och högerledet båda beräknar antalet sätt att forma en grupp med k personer varav två personer är ledare, ur en grupp av totalt n personer.

Tips. Du kan använda samma tips som för uppgift 3.

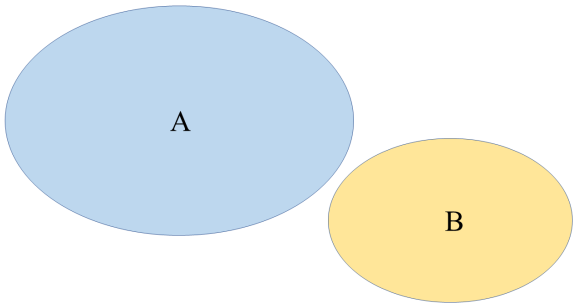
Lösning 5. 1. Det finns $|A| + |B| = 15 + 7 = 22$. stycken sätt att välja ett objekt från A eller ett objekt från B. Du kan beräkna detta med additionsregeln. Det beror på att det inte spelar någon roll om vi väljer ett objekt ur A eller ett ur B vilket gör att man kan tänka att man bara lägger ihop alla element i samma mängd och tar en. Antalet möjliga val är ju då bara det totala antalet element.

2. Det finns $|A||B| = 15 \cdot 7 = 105$ sätt att välja ett objekt från A och ett objekt från B. Detta gäller från multiplikationsregeln. Detta kan man se som att om vi tar upp ett element ur högen A finns det nu exakt $|B|$ val ur B. Detta gäller för alla element i A vilket gör att vi kan multiplicera med antalet i B och det ger det totala antalet kombinationer.

3. Det är antalet sätt vi kan välja ett objekt ur A och ett objekt ur B, alltså $15 \cdot 7 = 105$. Detta är den notation som används för att beskriva multiplikationsregeln, det är därför vi egentligen gör samma sak här som i förra uppgiften.

4. Det är antalet sätt att välja ett objekt ur A eller ett objekt ur B, alltså $15 + 7 = 22$. Detta är den notation som används för att beskriva multiplikationsregeln.

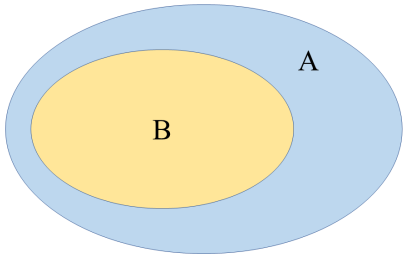
5. Det största värdet $A \cup B$ kan anta är $15 + 7 = 22$. I detta fallet (största möjliga unionen) kommer alla element i B vara olika från alla element i A, vilket gör att vår nya mängd kommer innehålla alla 7 element i B och alla 15 element i A.



Figur 5: $A \cup B$ blir som störst när de, såsom i figuren, är disjunkta.

Det minsta värdet $A \cup B$ kan anta är 15. I detta fallet (minsta möjliga unionen) kommer alla element i B vara närvarande i A. Alltså kommer vår nya mängd vara lika med mängden A, eftersom B också är närvarande i den mängden.

6. Det största värdet som $A \cap B$ kan anta är 7. I detta faller kommer alla element i B vara närvarande i A, såsom i figur 6. Alltså kommer $A \cap B = B$, och vi får med alla element i B.



Figur 6: $A \cup B$ blir som minst när B ligger i A.

Det minsta värdet som $A \cap B$ kan anta är 0. I detta fallet så kommer alla element i B vara skilda från alla element i A och vårt snitt kommer då bli en tom mängd, såsom i figur 5.

Tips. 1. I sådana uppgifter är det bra att fundera över hur additionsregeln och multiplikationsregeln kan appliceras.

2. Rita upp mängderna och de olika fallen, ligger mängderna i varandra (innehåller samma element), ligger de utanför varandra (innehåller inte samma element) eller ligger de delvis i varandra/utanför varandra?

Lösning 6. a) Additionsregeln ger att det finns $5 + 7 = 12$ sätt att välja en slips att ha på sig på intervjun.

b) Vi kan välja fritt mellan de seriösa slipsarna och de med komiskt tryck. Alltså hur många sätt kan man välja två slipsar från tolv stycken slipsar. Det blir antalet kombinationer

$$\binom{12}{2} = \frac{12!}{2!(12-2)!} = \frac{12!}{2! \cdot 10!} = \frac{12 \cdot 11}{2} = 66.$$

c) Svaret ges av multiplikationsregeln, då vi vill veta hur många sätt vi kan välja en slips från mängden av seriösa slipsar och en slips från mängden av komiska slipsar.

$$5 \cdot 7 = 35.$$

Tips. Tipsen till övning 5 gäller även för övning 6.

Referenser

Randall Munroe. Unsolved math problems. `https://xkcd.com/2529/`.

Föreläsning 2: Kombinatoriska bevis, binomialsatsen, kompositioner, och multinomialsatsen · 1MA020

Vilhelm Agdur[1]

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

17 januari 2023

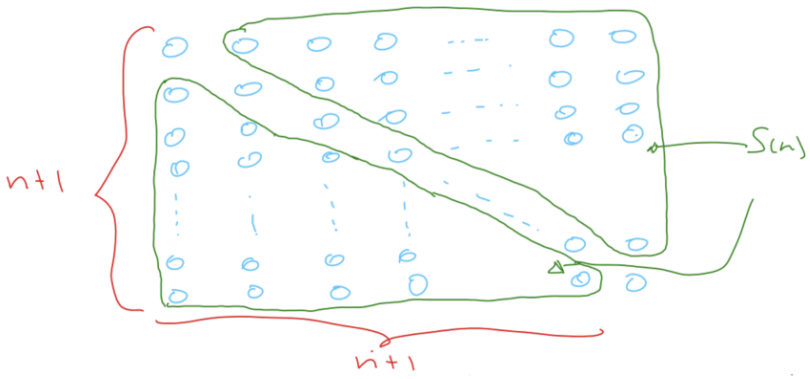
Vi fortsätter på förra föreläsningens idéer om kombinatoriska bevis och att räkna saker på två olika sätt. Sedan tillämpar vi detta på att bevisa binomialsatsen. Vi fortsätter med att diskutera omordningar och kompositioner, från vilket vi härleder *multi*nomialsatsen.

Kombinatoriska bevis

I slutet av förra föreläsningen diskuterade vi kombinatoriska bevis, och bevisade saker genom att räkna samma sak på två olika sätt. I denna föreläsningen fortsätter vi på det spåret, med fler bevis där vi hittar smarta sätt att räkna något.

Exempel 1. För $n \geq 0$, låt $S(n) = \sum_{k=1}^{n} k$. Vi vill bevisa att $S(n) = \frac{n(n+1)}{2}$.[2]

Vi studerar ett rutnät av $(n+1) \times (n+1)$ punkter, såsom i figuren.



Figur 1: Ett rutnät av punkter. Figur tagen direkt från förra årets föreläsningsanteckningar.

Vi ser på den nedre gröna triangeln, och försöker räkna antalet punkter i den. Vi ser att den vänstra kolumnen har $(n+1) - 1 = n$ punkter, den näst vänstraste har $(n+1) - 2 = n - 1$ punkter, och så vidare till den näst längst till höger som har en punkt, och kolumnen längst till höger har noll punkter i den gröna triangeln.

Alltså, om vi summerar över kolumnerna så får vi att det är totalt $n + (n-1) + \ldots + 2 + 1 = S(n)$ punkter i triangeln. Eftersom kvadraten så klart är helt symmetrisk är det lika många punkter i den övre gröna triangeln, och det är lätt att se att det är $n+1$ punkter på diagonalen.

[2] Det sägs att den store matematikern Carl Friedrich Gauss en gång fick uppgiften att räkna ut $1 + 2 + \ldots + 100$ av en lat mellanstadielärare som ville hålla sina elever upptagna i en stund, och förbluffade sin lärare genom att hitta svaret på bara några sekunder och utan papper och penna.

Han använde dock en annan metod än den vi använder, som inte involverade någon figur. Kan du komma på fler sätt att göra detta? (Eller Googla "Gauss triangular numbers story" om du bara vill veta svaret.)

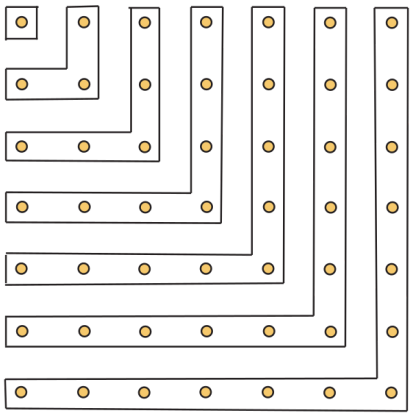
Alltså måste det totala antalet punkter i kvadraten vara $2S(n) + (n+1)$ – men vi vet också, så klart, att det är $(n+1)^2$. Så om vi löser detta för $S(n)$ får vi att

$$S(n) = \frac{(n+1)^2 - (n+1)}{2} = \frac{(n+1)((n+1)-1)}{2} = \frac{n(n+1)}{2}$$

precis som vi önskade.

Exempel 2. Vad är summan av de första n udda talen, det vill säga $\sum_{k=1}^{n} 2k-1$?

Svaret är n^2, som kan ses av nedanstående figur.



Figur 2: Bevis att summan av de första n udda talen är n^2. Bilden är tagen ur vår kursbok.

Exempel 3. Bevisa att $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Bevis. Vi bevisar detta genom att bevisa att både vänster och höger led räknar antalet delmängder till en mängd av n element, oavsett delmängdernas storlek.[3]

För vänster led kan vi observera att antalet delmängder oavsett storlek är summan av antalet delmängder av varje given storlek. Vi vet sedan innan att en delmängd av storlek k av en mängd av storlek n kallas en kombination, och det finns $\binom{n}{k}$ stycken sådana. Alltså är det totala antalet delmängder $\sum_{k=0}^{n} \binom{n}{k}$, som önskat.

För höger led använder vi multiplikationsregeln. För varje element i vår mängd har vi två val – antingen tar vi med elementet, eller inte – och vi har totalt n stycken element för vilka vi behöver göra detta val. Så om vi multiplicerar antalet val vi har varje gång får vi $2 \cdot 2 \cdot \ldots \cdot 2 = 2^n$ stycken delmängder, som önskat. □

[3] Man kan också betrakta detta som att vi räknar antalet binära strängar av längd n på två sätt, eftersom det finns en enkel bijektion mellan sådana och delmängder till en mängd X av storlek n.

Specifikt så fixerar vi en numrering av elementen av X, och säger att givet en binär sträng $x_1 x_2 \ldots x_n$ så får vi en delmängd $A \subseteq X$ genom att det första elementet av X ligger i A om $x_1 = 1$, det andra om $x_2 = 2$, och så vidare. På motsvarande sätt kan vi konstruera en binär sträng givet en delmängd.

Proposition 4 (Pascals Identitet)**.** *För $1 \leq k \leq n$ gäller det att*[4]

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

[4] Den här likheten säger exakt att Pascals triangel faktiskt innehåller binomialkoefficienterna.

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
 & 1 & & 5 & & 10 & & 5 & & 1 \\
 & & 1 & & 6 & & 15 & & 6 & & 1 \\
 & & & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}$$

Algebraiskt bevis.

$$\begin{aligned}\binom{n-1}{k-1}+\binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!}+\frac{(n-1)!}{k!((n-1)-k)!}\\ &= (n-1)!\left(\frac{k}{k!(n-k)!}+\frac{(n-k)}{k!(n-k)!}\right)\\ &= (n-1)!\frac{k+(n-k)}{k!(n-k)!}\\ &= \frac{n!}{k!(n-k)!}=\binom{n}{k}.\end{aligned}$$

□

Kombinatoriskt bevis. Låt X vara en mängd av storlek n. Vi vet att $\binom{n}{k}$ räknar antalet delmängder av storlek k till X. Låt oss komma på ett annat sätt att räkna antalet delmängder av storlek k, och se att det ger oss höger led.

Välj ett godtyckligt element $x \in X$. För varje delmängd A till X så innehåller den antingen x, eller så gör den inte det. För att skapa oss en delmängd A av storlek k som innehåller x lägger vi först in x i A, och sedan lägger vi till ytterligare $k-1$ element från de återstående $n-1$ elementen. Antalet sätt att göra det vet vi är precis $\binom{n-1}{k-1}$

Om vi i stället vill ha en delmängd A som *inte* innehåller x så kan vi fritt välja k element av de återstående $n-1$ elementen. Antalet sätt att göra det på vet vi är $\binom{n-1}{k}$.

Så additionsprincipen säger oss att antalet sätt att välja en delmängd som innehåller x eller inte innehåller x – vilket ju är alla delmängder – måste vara summan, alltså $\binom{n-1}{k-1}+\binom{n-1}{k}$, såsom önskat. □

Binomialsatsen

Teorem 5 (Binomialsatsen)**.** *För varje heltal $n \geq 0$ gäller det att*[5]

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$$

Bevis. Studera uttrycket

$$(x+y)^n = (x+y)(x+y)\dots(x+y).$$

Vad är det vi gör när vi expanderar ut detta uttrycket? Jo, vi väljer för varje parentes om vi tar ett x eller ett y – eller uttryckt i kombinatoriska termer, vi bildar ett ord ur alfabetet $\{x, y\}$. Så för $n = 3$ får vi till exempel att

$$(x+y)(x+y)(x+y) = xxx+xxy+xyy+yxx+yxy+yyy.$$

[5] Lägg märke till att vi inte är så precisa kring vad x och y är. I versionen ni lärde er i gymnasiet är de två reella tal, men egentligen är det här en likhet mellan polynom, som gäller mycket mer allmänt. Vi använder ju inte några specifika egenskaper hos de reella talen i det här beviset, bara räkneregler för polynom. När ni läser en kurs i algebra kommer ni se hur generellt den sortens räkningar fungerar.

Sedan kommer vi ihåg att multiplikation är kommutativt, så $xyy = yxy$. Alltså spelar det ingen roll i vilken ordning vi gjorde valen, bara hur många gånger vi valde x och hur många gånger vi valde y.[6]

Så antalet gånger vi får en term som är lika med $x^{n-k}y^k$ kommer alltså vara antalet $\{x, y\}$-strängar med k stycken y. Det antalet är så klart samma som antalet sätt att välja k platser att skriva y ur den totala mängden av n platser – det vill säga $\binom{n}{k}$.

Vi har alltså sett att koefficienten framför $x^{n-k}y^k$ när vi förenklat uttrycket kommer att vara $\binom{n}{k}$. Eftersom detta argument fungerar för varje k har vi bevisat satsen. □

[6] Alltså, formulerat på ett annat sätt, etiketterna av "när valdes vilken" spelar ingen roll.

Exempel 6. Ge ett algebraiskt och ett kombinatoriskt bevis för att

$$3^n = \sum_{k=0}^{n} \binom{n}{k} 2^k.$$

Kombinatoriskt bevis. Låt oss räkna antalet ternära strängar[7] av längd n på två olika sätt. Det enkla sättet är att använda multiplikationsprincipen – för varje bokstav har vi tre val, och vi behöver välja n gånger, alltså blir produkten av antalet val för varje gång 3^n.

[7] Det vill säga strängar med alfabetet $\{0, 1, 2\}$.

Ett annat sätt att räkna detta är att dela upp efter hur många ettor ordet innehåller. Först väljer vi antalet ettor, sedan väljer vi var ettorna skall stå, och till sist väljer vi vad resten av bokstäverna skall vara för något.

Givet att vi vet att vi skall ha k stycken ettor, och vi vet var de skall stå, så har vi $n - k$ bokstäver kvar att göra ett val för – och nu har vi bara två val, eftersom vi inte får välja ettor utan bara nollor och treor. Så enligt multiplikationsprincipen multiplicerar vi antalet val vi har i varje fall och får att det finns 2^{n-k} sätt att fylla i resten av ordet med nollor och treor.

Givet att vi vet att vi skall ha k stycken ettor, hur många olika strängar kan vi skapa? Antalet sätt att välja var ettorna skall stå är precis antalet kombinationer av k element från mängden av platser, $[n]$, och vi vet att det är $\binom{n}{k}$. När vi väl valt var ettorna skall stå kan vi fylla i resten på 2^{n-k} sätt, som vi såg i föregående stycket, så multiplikationsprincipen ger oss att det måste finnas $\binom{n}{k}2^{n-k}$ strängar av längd n med k stycken ettor.

Till slut vet vi att det totala antalet ternära strängar måste vara summan av detta över alla k, enligt additionsprincipen. Så om vi summerar detta får vi att det finns

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

ternära strängar. Efter att ha tillämpat likheten $\binom{n}{k} = \binom{n}{n-k}$ och vänt på indexeringen i summan ser vi att detta är precis höger led i ekvationen vi gav. □

Algebraiskt bevis. Vi använder binomialsatsen och ser att

$$\begin{aligned} 3^n &= (1+2)^n \\ &= \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 2^k = \sum_{k=0}^{n} \binom{n}{k} 2^k. \end{aligned}$$

□

Omordningar

Definition 7. En omordning[8] av en X-sträng s är en annan X-sträng s' där varje element i X förekommer lika många gånger i s' som i s. Specifikt måste alltså s och s' vara av samma längd.

[8] Engelska *rearrangement*, det verkar inte finnas ett helt inarbetat svenskt ord för detta, så omordning får fungera, om än klumpigt.

Exempel 8. Det finns sex omordningar av $ABBA$:

$$ABBA, ABAB, AABB, BAAB, BABA, BBAA.$$

Proposition 9. *Om s är en binär sträng av längd n med k stycken ettor finns det $\binom{n}{k}$ stycken omordningar av s.*

Bevis. Vi behöver helt enkelt räkna antalet binära strängar av längd n som har k stycken ettor. För att konstruera en sådan behöver vi helt enkelt välja på vilka platser det skall stå en etta – alltså välja en delmängd av k platser av de totalt n platserna. Detta vet vi att vi kan göra på $\binom{n}{k}$ sätt. □

Kompositioner

Antag att vi vill fördela ut n stycken osärskiljbara objekt bland k särskiljbara människor.

Exempel 10. Tre stycken lärare konkurrerar om två stycken äpplen de har fått av sina elever. På hur många olika sätt kan äpplena fördelas ut?

Här är $n = 3$ och $k = 2$. Det finns sex olika sätt:

Äpplen för A	Äpplen för B	Äpplen för C
2	0	0
1	1	0
1	0	1
0	2	0
0	1	1
0	0	2

Proposition 11. *Det finns $\binom{n+k-1}{k-1} = \binom{n+k-1}{n}$ sätt att fördela n osärskiljbara föremål mellan k särskiljbara personer.*

Bevis. Metoden för det här beviset brukar kallas för ett pinnar-och-stjärnor-argument.[9]

Vi studerar ord ur alfabetet $\{*, |\}$ med $k-1$ stycken pinnar och n stycken stjärnor. Till exempel om $n = 6$ och $k = 5$

$$**||*|*|**.$$

Vi tolkar detta ordet som en fördelning av föremål till personer såsom följer: Person ett får alla stjärnor innan första strecket, person två alla mellan första och andra strecket, och så vidare, tills person k får alla stjärnor efter det sista strecket. I vårt exempel får alltså person ett två föremål, person två inga, person tre och fyra ett var, och person fem får två.

Detta etablerar en bijektion mellan våra ord och fördelningarna till personer. Vi vet från Proposition 9[10] hur man räknar antalet sådana ord – våra ord har längd $n+k-1$ (de innehåller n stjärnor och $k-1$ streck) och $k-1$ av dem är av ena typen, så det måste finnas totalt $\binom{n+k-1}{k-1}$ ord, och alltså lika många fördelningar. □

Exempel 12. Hur många lösningar har ekvationen $x+y+z = 15$, ifall vi kräver att x, y, och z alla skall vara positiva heltal?

Vi kan se det här som en variant av problemet med att fördela osärskiljbara objekt mellan särskiljbara personer, där objekten är ettor och personerna är våra tre variabler.

Vi börjar med att ge varje variabel en etta, eftersom alla måste vara större än noll. Sedan har vi tolv ettor kvar att fördela mellan tre variabler, så Proposition 11 säger oss att det finns $\binom{12+3-1}{3-1} = \binom{14}{2} = 91$ lösningar.

Definition 13. I allmänhet är antalet sätt att skriva n som en summa av ett godtyckligt antal positiva heltal, där ordningen vi skrivar summan i spelar roll[11], antalet *kompositioner*[12] av n. Vi studerade alltså just antalet kompositioner av längd 3 av 15.

Multinomialkoefficienter

Exempel 14. Hur många omordningar finns det av ordet *SPAPASTA*?[13]

Det har 2 stycken S och P, 3 stycken A, och ett T. Vi kan skapa en omordning av detta ordet genom att först välja var vi placerar Ana – det kan vi göra på $\binom{8}{3}$ sätt, eftersom vi har åtta platser och tre An. När vi placerat ut dem har vi $8-3 = 5$ sätt att placera ut våra två S, så vi har $\binom{5}{2}$ val för hur vi gör det.

Likaledes har vi $\binom{3}{2}$ sätt att placera ut våra Pn, och till slut $\binom{1}{1}$ enda

[9] Engelska *stars and bars argument*.

[10] Den propositionen handlar om binära strängar, men vi har alfabetet $\{*, |\}$ – det spelar så klart ingen roll för antalet vad vi kallar våra bokstäver.

[11] $1+4$ och $4+1$ är alltså olika kompositioner av 5.

[12] Inte att blanda ihop med *kombinationer*, trots ordens snarlikhet.

[13] Ursprungligen ville jag ha det rimligare ordet *pastaså*s, men LaTeX gillar visst inte *Å* i ekvationer.

sätt att placera ut vårt T. Sammantaget blir det alltså

$$\begin{aligned}\binom{8}{3}\binom{5}{2}\binom{3}{2}\binom{1}{1} &= \frac{8!}{3!5!}\frac{5!}{2!3!}\frac{3!}{2!1!}\frac{1!}{1!0!} \\ &= \frac{8!}{3!2!2!1!}\end{aligned}$$

Definition 15. För varje heltal n och varje samling av heltal $k_1, k_2, \ldots, k_r$ sådana att $k_1 + k_2 + \ldots + k_r = n$ betecknar vi *multinomialkoefficienten* med

$$\binom{n}{k_1, k_2, \ldots, k_r} = \frac{n!}{k_1!k_2!\ldots k_r!}.$$

Notera att våra vanliga binomialkoefficienter är specialfallet när $r = 2$,

$$\binom{n}{k} = \binom{n}{k, n-k} = \binom{n}{n-k}.$$

Proposition 16. *Antag att s är en X-sträng av längd n, som innehåller k_1 stycken x_1, k_2 stycken x_2, och så vidare, upp till k_r stycken x_r – så $k_1 + k_2 + \ldots k_r = n$. Antalet omordningar av s ges av multinomialkoefficienten $\binom{n}{k_1, k_2, \ldots, k_r}$.*

Bevis. Låt R vara antalet omordningar av s. Vi använder återigen "räkna samma sak på två olika sätt"-metoden. Den här gången är vad vi vill räkna antalet permutationer av längd n ur alfabetet[14]

$$\begin{aligned}X' = \{&x_1^1, x_1^2, \ldots, x_1^{k_1}, \\ &x_2^1, x_2^2, \ldots, x_2^{k_2}, \\ &\vdots \\ &x_r^1, x_r^2, \ldots, x_r^{k_3}\}.\end{aligned}$$

Eftersom X' har exakt n bokstäver vet vi att antalet permutationer av det alfabetet är precis $n!$.

Låt oss nu räkna på ett mer komplicerat sätt. Vi kan också skapa oss en permutation av X' genom att först välja en omordning av s, och sedan välja ett sätt att sätta etiketter på bokstäverna i den omordningen.[15]

Om vi bara studerar våra x_1 i omordningen av s så har vi k_1 stycken, och vi skall sätta etiketter mellan 1 och k_1 på dem. Det kan vi göra på $k_1!$ sätt. Det samma gäller för varje annan bokstav, så multiplikationsprincipen säger oss att det totala antalet sätt att sätta etiketter måste vara $k_1!k_2!\ldots k_r!$. Det totala antalet permutationer av X' måste alltså vara R, antalet omordningar, gånger detta, så vi har sett att

$$n! = Rk_1!k_2!\ldots k_r!$$

och om vi löser detta för R får vi precis den sökta satsen. □

[14] Så i fallet där vårt ord är $SPAPASTA$ blir

$$X' = \{S^1, S^2, P^1, P^2, A^1, A^2, A^3, T^1\}.$$

Vi tar helt enkelt varje bokstav och ger den en etikett, så att bokstäverna blir särskiljbara.

[15] Så vi väljer en omordning av $SPAPASTA$, till exempel $ASPTAPAS$, och sätter sedan etiketter på bokstäverna för att få till exempel $A^2S^1P^2T^1A^1P^1A^3S^2$, vilket är en permutation av X'.

Teorem 17 (Multinomialsatsen)**.** *Det gäller att*

$$(x_1 + x_2 + \ldots + x_r)^n = \sum_{\substack{k_1,k_2,\ldots,k_r \geq 0 \\ k_1+k_2+\ldots+k_r=n}} \binom{n}{k_1, k_2, \ldots, k_r} x_1^{k_1} x_2^{k_2} \ldots x_r^{k_r}$$

Bevis. Precis samma argument som för binomialsatsen fungerar här. □

Övningar

Övning 1. I Exempel 1 såg vi att

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

genom att studera en kvadrat av $(n+1) \times (n+1)$ punkter, och observera att den sökta summan räknar antalet punkter under diagonalen i figuren. Sedan använde vi ett algebraiskt argument för att få en formel för detta antal.

En uppmärksam läsare kanske lägger märke till att $\frac{n(n+1)}{2} = \binom{n+1}{2}$, vilket ju också räknar antalet kombinationer av två element ur en mängd av $n+1$ element. Kan du komma på ett *kombinatoriskt* bevis för varför antalet element under diagonalen på kvadraten är samma sak som antalet kombinationer av 2 element från en mängd av $n+1$ element?

Övning 2. I en sidnot till Exempel 3 nämnde vi att det också går att se problemet som att räkna binära strängar av längd n, via en bijektion mellan sådana och delmängder till en mängd.

Kan du skriva ett kombinatoriskt bevis för att $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ som resonerar om binära strängar istället för om delmängder till en mängd?

Övning 3. Hur många heltalslösningar finns det till $x + y + z = 43$, om vi kräver att $x \geq 1$, $y \geq 17$, och $z \geq 5$?

Övning 4. Hur många omordningar finns det av ordet 54240244?

Hur många omordningar finns det av det ordet som inte börjar med en nolla?

Övning 5. Hur många ternära strängar av längd $2n$ finns det, där ettorna bara får dyka upp på udda positioner?

Övning 6. Låt m och w vara positiva heltal. Ge ett kombinatoriskt bevis för att det, för varje $0 \leq k \leq m + w$, gäller att

$$\sum_{j=0}^{k} \binom{m}{j} \binom{w}{k-j} = \binom{m+w}{k}.$$

Föreläsning 3: Induktion, lådprincipen, och inklusion-exklusion · 1MA020

Vilhelm Agdur[1]

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

23 januari 2023

Vi börjar med att diskutera induktion och induktionsbevis. Sedan nämner vi lådprincipen och ger några tillämpningar av den. Till slut påbörjar vi vår diskussion av inklusion-exklusion.

Induktion

Axiom 1 (Induktion för heltalen)**.** [2]*Antag att $A \subseteq \mathbb{N}$ är någon mängd av heltal. Ifall*

1. *$1 \in A$, och*
2. *för varje n, om $n \in A$, så är också $n+1 \in A$,*

så är $A = \mathbb{N}$, det vill säga, alla heltal ligger i A.

[2] Är detta en sats eller ett axiom? Det beror på vilka axiom du väljer att ta, och hur exakt du definierar vad du menar med "heltalen".

Precis vilka axiom vi antar är inte något som vi skall gå in på i denna kursen, det hör snarare hemma i en kurs i logik. Vi nöjer oss att säga, i en sidnot för den intresserade, att enligt Peano är detta ett axiom, men om man resonerar i Zermelo-Fraenkel kan man bevisa att heltalen finns och har denna egenskap.

Man brukar ofta föredra att tänka på induktion som att det handlar om egenskaper hos eller påståenden om tal – då säger vi att vi har en egenskap ϕ, och om vi kan bevisa $\phi(1)$ och kan bevisa att $\phi(n) \to \phi(n+1)$, så följer det att $\forall n \phi(n)$.

Detta perspektiv är helt ekvivalent med det axiom vi just gav – om vi låter A vara mängden av tal med egenskapen ϕ, eller låter ϕ vara egenskapen "talet ligger i A".

Exempel 2. Bevisa att, för varje $n \geq 1$, $\sum_{i=0}^{n-1} 2^i = 2^n - 1$.

Bevis. Låt A vara mängden av alla n sådana att $\sum_{i=0}^{n-1} 2^i = 2^n - 1$.

Vi ser enkelt att $1 \in A$, eftersom påståendet då blir att $2^0 = 2^1 - 1$, vilket ju är sant.

Låt oss visa att om $n \in A$ så är också $n+1$ i A. Så vi antar likheten för n, och vill visa att $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$. Så om vi skriver vänster led i denna likheten och manipulerar den så ser vi att

$$\begin{aligned}\sum_{i=0}^{n} 2^i &= \sum_{i=0}^{n-1} 2^i + 2^n \\ &= (2^n - 1) + 2^n = 2 \cdot 2^n - 1 = 2^{n+1} - 1\end{aligned}$$

precis som önskat. Så induktionsprincipen ger oss att likheten håller för alla n. □

Exempel 3. Bevisa att det finns $n!$ permutationer av längd n från ett alfabete med n bokstäver.

Bevis. Att det finns exakt en permutation av längd ett från ett alfabete med en bokstav är uppenbart.

För induktionssteget, antag att vi vet att det finns $n!$ permutationer av längd n från alfabetet X, där $|X| = n$. Hur kan vi konstruera en permutation av längd $n+1$ från alfabetet $X \cup \{a\}$? Jo, vi börjar med att välja en permutation av X – vilket vi per induktionshypotesen kan göra på $n!$ sätt – och väljer sedan var vi skall stoppa in a. Vi har $n+1$ alternativ för plats för a, så enligt multiplikationsprincipen har vi $(n+1)n! = (n+1)!$ sätt att skapa en permutation av vårt nya längre alfabete. □

Kommentar 4 (Stark induktion). I själva verket kan vi ta som induktionshypotes inte bara att $n \in A$, utan att $[n] \subseteq A$, det vill säga att alla heltal från 1 till n ligger i A. (Eller "har egenskapen ϕ", om vi föredrar den formuleringen.)

Att göra det antagandet kallas för *stark induktion* – vilket egentligen är ett missvisande namn, eftersom det är ekvivalent med vanlig induktion, och alltså kan bevisa precis samma saker. Den är alltså inte ett dugg starkare i logisk mening – men ibland ger den snyggare formuleringar av bevisen.

Teorem 5 (Välordningsprincipen)**.** *För varje mängd $A \subseteq \mathbb{N}$ är antingen A tom, eller så har A ett minsta element.*[3]

[3] Vi väljer att formulera det här som en sats som följer av induktionsprincipen – i kursboken är de två separata påståenden, och förra årets anteckningar går i motsatt riktning och bevisar induktion baserat på välordning.S

Bevis. Antag att A är en mängd av heltal utan minsta element – vi bevisar med (stark) induktion att $A = \emptyset$, genom att bevisa att $A^c = \mathbb{N}$.

Att $1 \in A^c$ är uppenbart – ett är det minsta heltalet, så vore ett i A vore det trivialt ett minsta element i A.

Antag nu att $1, 2, \ldots, n \in A^c$. Alltså är inga av heltalen innan $n+1$ med i A, så om $n+1$ vore i A skulle det vara As minsta element. Så eftersom A inte har ett minsta element kan inte $n+1$ ligga i A.

Alltså ger oss nu induktionsprincipen att $A^c = \mathbb{N}$, det vill säga $A = \emptyset$, såsom önskat. □

Kommentar 6. Detta ger upphov till en vanlig bevisteknik.[4] Antag att vi vill bevisa att alla heltal har en viss egenskap ϕ. Vi antar då, för motsägelse, att det inte är så – då måste det finnas ett minsta motexempel, enligt välordningsprincipen.

[4] På engelska kallad *proof by infinite descent*.

Sedan använder vi detta minsta motexempel för att konstruera ett ännu mindre motexempel, och får en motsägelse därur. Att vi kunde skapa ett mindre motexempel motsäger ju nämligen att det vi började med var det minsta exemplet.

Lådprincipen

Teorem 7 (Lådprincipen). [5] *Om vi har m stycken objekt som skall fördelas i n lådor, och $m > n$, så kommer någon låda behöva innehålla mer än ett objekt.*

Exempel 8. Om det finns tretton studenter i rummet måste åtminstone två av dem fylla år i samma månad. Här är studenterna objekten och årets månader lådorna.[6]

Teorem 9 (Generaliserade lådprincipen). *Om vi har m objekt som skall fördelas i n lådor, och $m > kn$, så måste åtminstone en av lådorna innehålla minst $k + 1$ objekt.*

Exempel 10. Om det finns tjugofem studenter i rummet måste det finnas minst en månad i vilken tre eller fler av dem fyller år.

Exempel 11. Antag att fem punkter placeras i en liksidig triangel med sidlängd ett. Då finns det två punkter vars avstånd mellan varandra är högst $\frac{1}{2}$.

Dela upp triangeln i fyra bitar, enligt figuren. Lådprincipen säger

oss att det måste finnas en av dessa bitar som innehåller minst två punkter. Men om de ligger i samma bit måste deras avstånd mellan varandra vara högst $\frac{1}{2}$.

Exempel 12. För varje mängd av fem punkter på en sfär finns det ett halvklot som innehåller minst fyra av punkterna.

Välj två av de fem punkterna godtyckligt och rita storcirkeln som passerar genom dem. Denna delar upp jorden i två halvklot, så lådprincipen säger oss att ett av dessa halvklot måste innehålla minst två av de återstående tre punkterna. Det halvklotet har alltså de två punkterna vi ritade storcirkeln genom och minst två punkter till, för totalt minst fyra.

Exempel 13. I varje grupp av sex personer finns det antingen en grupp av tre personer som alla är vänner eller en grupp av tre personer som alla inte är vänner.[7]

Välj en godtycklig person i gruppen. Enligt lådprincipen måste det antingen finnas tre personer som hon inte är vän med, eller tre personer som hon är vän med.

[5] Också kallad Dirichlets lådprincip, efter den tyske matematikern Peter Gustav Lejeune Dirichlet. Eller på engelska "the pigeonhole principle" – vilket onekligen är ett mer målande namn än vår svenska lådprincip.

[6] Här önskar jag att kursen gick på engelska, så jag kunde skriva, såsom i förra årets anteckningar, att "students are pigeons".

Figur 1: Figur tagen från förra årets föreläsningsanteckningar.

[7] Vi antar här att "är vänner"-relationen är symmetrisk, det vill säga att om jag är vän med dig är du vän med mig. Förhoppningsvis är det antagandet sant på universitetet, även om det inte var sant i mellanstadiet.

Ifall det finns tre personer som hon inte är vän med har vi två fall – antingen är alla tre vänner med varandra, i vilket fall vi är klara, eller så finns det ett par av dem som inte känner varandra. Men i så fall bildar det paret, tillsammans med vår första person, en grupp av tre personer som alla inte känner varandra.

Ifall det finns tre personer som hon är vän med resonerar vi på samma vis. Antingen är ingen av de tre personerna vänner med varandra, i vilket fall vi hittat vår grupp, eller så finns det ett par som känner varandra, och i så fall bildar det paret tillsammans med vår första person en triangel som känner varandra.

Vad vi just studerat är det enklaste fallet av Ramseys sats.[8] Låt oss definiera en lite mer allmän version av problemet.

[8] Namngiven efter Frank P. Ramsey, som var en fascinerande person som hann bli vän med Wittgenstein och Keynes och finna viktiga resultat inom ekonomi, matematik, och filosofi innan sin bortgång vid 26 års ålder.

Definition 14. För varje par av positiva heltal r och s är $R(r,s)$ det minsta antalet personer man behöver bjuda in på en fest för att det skall finnas antingen en grupp av r personer som alla känner varandra, eller en grupp av s personer där ingen känner någon annan i gruppen.[9]

[9] Eller mer formellt, formulerat i termer av grafer: (Vi har inte introducerat sådana än, men nästan hälften av er har ju läst kursen i grafteori.)
$R(r,s)$ är det minsta talet sådant att varje graf G med minst $R(r,s)$ noder antingen innehåller en inducerad kopia av K_r eller har en inducerad kopia av K_s i G^c, komplementgrafen till G.

Vad Exempel 13 visade är alltså att $R(3,3) = 6$. Vad Ramseys sats säger i allmänhet är att $R(r,s)$ är ändligt.[10]

[10] Problemet att beräkna exakt vad $R(r,s)$ är är extremt svårt – vi vet att $R(4,4) = 18$, men kan inte bestämma $R(5,5)$ mer exakt än att det är mellan 43 och 48.

Teorem 15 (Ramseys sats)**.** *För varje $r,s \geq 1$ är $R(r,s) < \infty$.*

Teorem 16 (Erdős-Szekeres)**.** *För alla $r,s \geq 1$ gäller det att varje följd av $(r-1)(s-1)+1$ distinkta reella tal antingen innehåller en ökande delföljd av längd r eller en minskande delföljd av längd s.*

Bevis. Kalla vår talföljd $n_1, n_2, \ldots, n_{(r-1)(s-1)+1}$. Ge varje n_i en etikett (a_i, b_i) som följer: a_i är längden av den längsta ökande delföljden som slutar i n_i, och b_i är längden av den längsta minskande delföljden som slutar i n_i.[11]

[11] Här menar vi med "slutar i" inte att de inte kan fortsättas längre med något n_j för $j > i$, bara att vi mäter längden av följderna fram till i.

Vi hävdar att alla tal n_i får distinkta etiketter. Överväg paret n_i, n_j för $i < j$ – om $n_i < n_j$ kan vi fortsätta den längsta ökande delföljden som slutar i n_i genom att lägga till n_j, så $a_j \geq a_i + 1$. Likaledes, om $n_i > n_j$ kan vi fortsätta den längsta minskande delföljden som slutar i n_i genom att lägga till n_j, så $b_j \geq b_i + 1$.

Antag nu för motsägelse att det inte finns någon ökande delföljd av längd r, och ingen minskande delföljd av längd s. Då måste $1 \leq a_i \leq r-1$ och $1 \leq b_i \leq s-1$ för alla i.[12]

[12] $a_i, b_i \geq 1$ eftersom n_i självt är en delföljd som är både minskande och ökande.

Alltså finns det $(r-1)(s-1)$ tillgängliga etiketter att tilldela till $(r-1)(s-1)+1$ stycken objekt, och alla objekten måste få distinkta etiktter. Lådprincipen säger oss att detta är omöjligt, och vi har vår motsägelse. □

Inklusion-exklusion

I matematiska institutionens fikarum för de anställda brukar det finnas äpplen, klementiner, och bananer i fruktlådorna. Om någon säger dig att det för tillfället finns femton runda frukter och tio frukter som inte går att odla i Sverige i lådorna, kan du räkna ut hur många frukter det finns?

Det kan du förstås inte – problemet är att en klementin tillhör båda kategorierna, så om det finns tio klementiner finns det totalt femton frukter (tio klementiner och fem äpplen), men om det finns noll klementiner finns det totalt tjugofem frukter (femton äpplen och tio bananer). Utan informationen om hur många klementiner det finns kan svaret på frågan variera.

Om vi låter A vara mängden av runda frukter och B vara mängden av frukter som inte kan odlas i Sverige är vad vi har observerat att[13]

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

En dag kommer en administratör på idén att citroner faktiskt också är en frukt, och berättar för dig att idag finns det tio runda frukter, elva som inte kan odlas i Sverige, och sju *gula frukter*. Du blir förvirrad och går hem och ritar ett Venndiagram över frukter.[14]

Formeln du kommer på efter att ha studerat ditt Venndiagram är att

$$\begin{aligned}|A \cup B \cup C| = |A| + |B| + |C| \\ - |A \cap B| - |A \cap C| - |B \cap C| \\ + |A \cap B \cap C|.\end{aligned}$$

Innan den fruktgalna administratören hinner lägga till ännu en absurd kategori av frukt undsätter dig din kombinatoriklärare med följande sats:

Teorem 17 (Inklusion-exklusion)**.** *För varje samling av mängder $A_1, \dots, A_n$ gäller det att*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \left(\sum_{\substack{I \subseteq [n] \\ |I|=k}} \left|\bigcap_{i \in I} A_i\right| \right),$$

[13] Jämför detta med additionsprincipen, som i en formulering säger att $|A \coprod B| = |A| + |B|$. När vi introducerade den var vi noggranna med skillnaden mellan $\coprod$ och $\cup$, och sade att vi skulle återkomma till vad som händer om A och B kan dela element.
Detta är vår återkomst.

[14] Nästa morgon får du reda på att det nu dessutom finns gula äpplen, päron, stjärnfrukt, och Xoconostler. Du skriver en arg insändare i UNT om vad universitetet egentligen lägger sin budget på.

eller, uttryckt mindre kompakt, att

$$\begin{aligned}\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n}|A_i| \\ &- \sum_{\{i,j\}\in[n]} \left|A_i \cap A_j\right| \\ &+ \sum_{\{i,j,k\}\in[n]} \left|A_i \cap A_j \cap A_k\right| \\ &- \dots \\ &+ (-1)^{n-1}|A_1 \cap A_2 \cap \dots \cap A_n|.\end{aligned}$$

Innan vi bevisar detta behöver vi definiera ett väldigt nyttigt verktyg som vi kommer använda i beviset.

Definition 18. Antag att $A \subseteq X$ är två mängder. Vi definierar *indikatorfunktionen* $\mathbb{1}_A : X \to \{0,1\}$ *för mängden* A som

$$\mathbb{1}_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A. \end{cases}$$

Den är alltså ett om och endast om dess argument ligger i A. Vi kan observera några grundläggande egenskaper hos dessa funktioner:

- $\mathbb{1}_A(x)\mathbb{1}_B(x) = \mathbb{1}_{A\cap B}(x)$
- $1 - \mathbb{1}_A(x) = \mathbb{1}_{X\setminus A}(x)$
- $|A| = \sum_{x\in A} \mathbb{1}_A(x)$
- $(\mathbb{1}_A(x))^n = \mathbb{1}_A(x)$ för alla $n \neq 0$.

Med denna definition gjord kan vi nu resonera algebraiskt om mängder och deras kardinalitet, och kan alltså ge ett algebraiskt bevis av inklusion-exklusion-principen.

Algebraiskt bevis av Teorem 17. Låt $X = \cup_{i=1}^{n} A_i$. Vi ser att

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{x\in X} \mathbb{1}_X(x)$$

så vi kan fokusera på varje punkt i taget, och visa att den räknas rätt antal gånger.

Studera nu uttrycket

$$(\mathbb{1}_X(x) - \mathbb{1}_{A_1}(x))(\mathbb{1}_X(x) - \mathbb{1}_{A_2}(x)) \dots (\mathbb{1}_X(x) - \mathbb{1}_{A_n}(x))$$

och observera att det måste vara identiskt noll. För varje element $x \in X$ ligger ju i något A_i, så produkten innehåller en term $\mathbb{1}_X(x) - \mathbb{1}_{A_i}(x) = 1 - 1 = 0$.

Vad får vi om vi multiplicerar ut detta uttrycket? Jo, vi får en term per mängd $I \subseteq [n]$, där vi valt sidan $\mathbb{1}_X(x)$ för $i \notin I$ och valt sidan $-\mathbb{1}_{A_i}(x)$ för $i \in I$.[15] Vi vet att uttrycket är noll, så vad vi får är likheten

$$\sum_{I \subseteq [n]} (\mathbb{1}_X(x))^{n-|I|} \prod_{i \in I} (-\mathbb{1}_{A_i}(x)) = 0$$

och om vi skriver termerna för $I = \emptyset$ och $I = [n]$ separat har vi likheten

$$\prod_{i=1}^{n} (-\mathbb{1}_{A_i}(x)) + \left(\sum_{\substack{I \subset [n] \\ \emptyset \neq I \neq [n]}} (\mathbb{1}_X(x))^{n-|I|} \prod_{i \in I} (-\mathbb{1}_{A_i}(x)) \right) + (\mathbb{1}_X(x))^n = 0$$

Vi vet av våra räkneregler för indikatorfunktioner att $\mathbb{1}_X(x)^{n-|I|} = \mathbb{1}_X(x)$, eftersom vi plockat ut termen där exponentn blir noll. Den återstående $\mathbb{1}_X(x)$ kan vi bli av med via en annan räkneregel – vi vet att $\mathbb{1}_X(x)\mathbb{1}_{A_i}(x) = \mathbb{1}_{X \cap A_i}(x) = \mathbb{1}_{A_i}(x)$, eftersom $A_i \subseteq X$, och vi kan göra detta eftersom vi plockat ut termen där vi inte har någon A_i att absorbera in den i.

Om vi tillämpar dessa förenklingar, flyttar ut minustecknet ur produkten och ser att $\mathbb{1}_X(x)^n = \mathbb{1}_X$, blir vad som återstår

$$(-1)^n \prod_{i=1}^{n} \mathbb{1}_{A_i}(x) + \sum_{\substack{I \subset [n] \\ \emptyset \neq I \neq [n]}} (-1)^{|I|} \prod_{i \in I} (\mathbb{1}_{A_i}(x)) + \mathbb{1}_X(x) = 0.$$

Nu kan vi flytta ihop första och andra termen under en summa, eftersom bägge inte innehåller någon $\mathbb{1}_X(x)$. Om vi gör det, och flyttar över den summan på andra sidan, så får vi att

$$\mathbb{1}_X(x) = \sum_{\substack{I \subseteq [n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left(\prod_{i \in I} \mathbb{1}_{A_i}(x) \right).$$

Om vi använder räkneregeln att $\mathbb{1}_A(x)\mathbb{1}_B(x) = \mathbb{1}_{A \cap B}(x)$ på produkten här och sedan summerar likheten över alla $x \in X$ så får vi att

$$\sum_{x \in X} \mathbb{1}_X(x) = \sum_{\substack{I \subseteq [n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left(\sum_{x \in X} \mathbb{1}_{\bigcap_{i \in I} A_i}(x) \right)$$

vilket, om vi använder oss av att $\sum_{x \in X} \mathbb{1}_A(x) = |A|$, blir

$$|X| = \sum_{\substack{I \subseteq [n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|$$

vilket vi någorlunda enkelt ser är ett annat sätt att skriva formeln vi var ute efter. □

[15] Jämför med hur vi resonerade om att multiplicera ut en produkt när vi bevisade binomialsatsen.

Exempel 19. Hur många heltalslösningar finns det till $x_1 + x_2 + x_3 = 20$, där $0 \leq x_1 \leq 8$, $0 \leq x_2 \leq 10$, och $0 \leq x_3 \leq 12$?

Låt

$$X = \left\{(x_1, x_2, x_2) \in \mathbb{Z}^3_{\geq 0} \;\middle|\; x_1 + x_2 + x_2 = 20\right\}$$

och låt

$$A_1 = \left\{(x_1, x_2, x_2) \in \mathbb{Z}^3_{\geq 0} \;\middle|\; x_1 + x_2 + x_2 = 20, x_1 > 8\right\},$$

$$A_2 = \left\{(x_1, x_2, x_2) \in \mathbb{Z}^3_{\geq 0} \;\middle|\; x_1 + x_2 + x_2 = 20, x_2 > 10\right\},$$

$$A_3 = \left\{(x_1, x_2, x_2) \in \mathbb{Z}^3_{\geq 0} \;\middle|\; x_1 + x_2 + x_2 = 20, x_3 > 12\right\}$$

vara mängder av *dåliga* lösningar, som inte uppfyller våra krav.

Vad vi vill göra är alltså att räkna ut $\left|(A_1 \cup A_2 \cup A_3)^c\right| = |X| - |A_1 \cup A_2 \cup A_3|$. Inklusion-exklusion säger oss att

$$\begin{aligned}|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| \\ - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ + |A_1 \cap A_2 \cap A_3|\end{aligned}$$

så vad vi behöver göra är att räkna ut $|X|$ och storleken på dessa snitten.

Vi såg redan i förra föreläsningen, i biten om omordningar, hur man räknar ut $|X|$ – det ges av $\binom{20+3-1}{3-1}$. För att räkna ut A_1 tänker vi att vi börjar med att ge nio mynt till x_1, och fördelar de återstående elva mynten godtyckligt. Vår formel ger oss att detta kan göras på $\binom{11+3-1}{3-1}$ sätt. Så, om vi tillämpar detta på alla tre mängderna ser vi att

$$|A_1| = \binom{11+3-1}{3-1}, \quad |A_2| = \binom{9+3-1}{3-1}, \quad |A_3| = \binom{7+3-1}{3-1}.$$

De större snitten är enklare att räkna ut – för $A_1 \cap A_2$ måste vi dela ut nio mynt till x_1, och sedan elva mynt till x_2, så vi har inga mynt kvar att dela ut fritt, och $|A_1 \cap A_2| = 1$. För de två andra snitten ser vi att $9 + 13 > 20$ och $11 + 13 > 20$, så de snitten måste vara tomma. Likaledes måste snittet av alla tre mängderna vara tomt.[16]

[16] Detta följer så klart också redan av observationen att $A_1 \cap A_3 = \emptyset$ – att snitta med en till mängd kan ju inte lägga till fler element.

Sätter vi tillbaka dessa talen i inklusion-exklusion-formeln ser vi att vi fått att

$$\begin{aligned}\left|(A_1 \cup A_2 \cup A_3)^c\right| &= |X| - |A_1 \cup A_2 \cup A_3| \\ &= \binom{20+3-1}{3-1} - \left(\binom{11+3-1}{3-1} + \binom{9+3-1}{3-1}\right. \\ &\qquad \left. + \binom{7+3-1}{3-1} - 1\right) \\ &= 63.\end{aligned}$$

Derangemang

Definition 20. Ett *derangemang*[17] av längd n är en permutation σ av längd n ur alfabetet $[n]$, sådan att $\sigma(k) \neq k$ för alla k.

[17] På engelska *derangement*.

Teorem 21. *Det finns*

$$n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$$

derangemang av längd n.[18]

[18] Ni kanske känner igen summan här som en partialsumma av Taylorexpansionen av e^x då $x = -1$ – så antalet derangemang är mycket nära $\frac{n!}{e}$ för stora n.

Bevis. Låt S_n vara mängden av alla permutationer av $[n]$ av längd n, och för varje i,

$$A_i = \{\sigma \in S_n \mid \sigma(i) = i\}$$

så att vi vill räkna antalet element i $S_n \setminus \bigcup_{i=1}^{n} A_i$.

Att $|S_n| = n!$ lärde vi oss redan första föreläsningen, och inklusion-exklusion ger oss att

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \left(\sum_{\substack{I \subseteq [n] \\ |I|=k}} \left|\bigcap_{i \in I} A_i\right| \right).$$

Så vad vi behöver göra är att lista ut vad $|\bigcap_{i \in I} A_i|$ är för varje givet $I \subseteq [n]$. Detta snittet blir precis mängden av permutationer sådana att $\sigma(i) = i$ för varje $i \in I$. Så för att skapa en sådan måste vi först sätta $\sigma(i) = i$ för dem, och sedan kan vi välja en ordning fritt för de återstående $n - k$ platserna. Detta kan vi alltså göra på $(n-k)!$ sätt.

För varje k finns det $\binom{n}{k}$ stycken mängder I, så sammantaget måste vi ha att

$$\begin{aligned}
\sum_{k=1}^{n} (-1)^{k-1} \left(\sum_{\substack{I \subseteq [n] \\ |I|=k}} \left|\bigcap_{i \in I} A_i\right| \right) &= \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! \\
&= \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!(n-k)!} (n-k)! \\
&= \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}
\end{aligned}$$

så att

$$\begin{aligned}
\left|S_n \setminus \bigcup_{i=1}^{n} A_i\right| &= |S_n| - \left|\bigcup_{i=1}^{n} A_i\right| \\
&= n! - \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!} = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}
\end{aligned}$$

såsom vi önskade visa. □

Övningar

Övning 1. Ge ett induktionsbevis av Teorem 17, teoremet där vi bevisar inklusion-exklusion-principen.

Övning 2. Antag att du äger svarta, gråa, blåa, och vita strumpor. Tyvärr är du väldigt oorganiserad, så du förvarar dem inte i par. Varje morgon sträcker du dig ner i din strumplåda och tar upp strumpor slumpmässigt, en i taget, tills du har ett matchande par av någon färg.

Hur många strumpor kan du som mest behöva plocka upp?

Övning 3. Man kan visa, med samma metod som vi använde i Exempel 13, att

$$R(r,s) \leq R(r-1,s) + R(r,s-1)$$

för alla $r, s \geq 2$.

Använd denna olikhet för att bevisa Ramseys sats, Teorem 15.[19]

Övning 4. Beteckna antalet derangemang av n med d_n. Ge ett kombinatoriskt bevis[20] för att

$$d_n = (n-1)(d_{n-1} + d_{n-2}).$$

Övning 5. Hur många heltalslösningar har ekvationen $x_1 + x_2 + x_3 + x_4 = 29$ om vi kräver $0 \leq x_i \leq 9$ för alla i?

Övning 6. Antag att den fruktgalna administratören i vårt exempel till slut introducerat tio olika kategorier av frukt. Hur många termer kommer formeln för inklusion-exklusion ha när $n = 10$?

[19] Ledtråd: Induktion. Vad kan basfallet tänkas vara?

[20] Ledtråd: För ett givet derangemang σ av längd n, låt k vara det tal som skickas till 1. Det finns två fall: Antingen är $\sigma(1) = k$ eller inte. Hur många derangemang finns det i varje fall?

Föreläsning 4: Sammanfattning av alla räkneproblem, samt cykler · 1MA020

Vilhelm Agdur[1]

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

30 januari 2023

Vi börjar med att räkna antalet surjektioner med hjälp av inklusion-exklusion. Sedan använder vi det för att räkna antalet mängdpartitioner.

Sedan skriver vi en stor tabell, och ser att merparten av alla de till synes disparata räkneproblem vi studerat faktiskt passar in i ett system.

Till slut disktuerar vi en jobbigare variant av problemet med människor som sitter runt ett runt bord, och använder denna för att introducera konceptet av cykler i en permutation.

Surjektioner

Definition 1. Låt A och B vara två mängder, och $f : A \to B$ en funktion. Vi definierar *bilden* av A som

$$f(A) = \{b \in B \mid \exists a \in A : f(a) = b\},$$

det vill säga alla element i B som träffas av något element i A under f.

Funktionen f är en *surjektion* om $f(A) = B$. Om det finns en surjektion från A till B gäller det att $|A| \geq |B|$.[2]

[2] Detta är uppenbart för ändliga mängder A och B – för oändliga mängder är detta definitionen av ordningen mellan kardinaltal.

Definition 2. För $n \geq m \geq 1$ ges *Stirlings partitionstal*, också kallat *Stirlingtalet av andra sorten*, av

$$\left\{ n \atop m \right\} = \frac{1}{m!} \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n.$$

Teorem 3. *Låt A och B vara ändliga mängder med $|A| = n$, $|B| = m$, och $n \geq m$. Antalet surjektioner från A till B ges av*

$$S(n,m) = m! \left\{ n \atop m \right\} = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n.$$

Bevis. Låt X vara mängden av alla funktioner från A till B, och för varje $b \in B$, låt X_b vara mängden av funktioner från A till B som inte träffar b. Vi vill, som vanligt, räkna ut $|X \setminus \bigcup_{b \in B} X_b| = |X| - |\bigcup_{b \in B} X_b|$.

Multiplikationsprincipen ger oss enkelt att $|X| = m^n$ – varje element i A har m val för var det skall skickas, och vi har n stycken element att göra det valet för.

Inklusion-exklusion ger oss att

$$\left| \bigcup_{b \in B} X_b \right| = \sum_{I \subseteq B} (-1)^{|I|+1} \left| \bigcap_{b \in I} X_b \right|$$

och vad vi behöver räkna är antalet funktioner från A till B som undviker att träffa en viss mängd I. Ett specialfall ser vi omedelbart – om $I = B$ måste snittet vara tomt, eftersom elementen i A måste skickas *någonstans*.

Att räkna dem är relativt enkelt – en funktion från A till B som inte träffar en viss mängd $I \subset B$ är ju precis en funktion från A till $B \setminus I$, och vi vet att det finns $|B \setminus I|^{|A|} = (m - |I|)^n$ sådana. Så vad vi får är att

$$\left| \bigcup_{b \in B} X_b \right| = \sum_{I \subset B, I \neq B} (-1)^{|I|+1} (m - |I|)^n,$$

där summan är över delmängder *inte lika med* B eftersom vi redan observerat att då $I = B$ blir det hela noll.

Så om vi grupperar den här summan efter storleken på I vet vi att det finns $\binom{m}{k}$ stycken val av I av storlek k (och nu vet vi att $I \neq B$, så storlek m är utesluten och summan går bara upp till $m - 1$), så

$$\left| \bigcup_{b \in B} X_b \right| = \sum_{k=0}^{m-1} (-1)^{k+1} \binom{m}{k} (m - k)^n$$

vilket ger oss resultatet, när vi stoppar in detta i $S(n, m) = |X| - |\bigcup_{b \in B} X_b|$. □

Exempel 4. Antag att en farmor stickat fem filtar åt sina tre barnbarn. På hur många sätt kan hon fördela filtarna, så att varje barn får åtminstone en filt? Eftersom de är handstickade är så klart filtarna *särskiljbara*, så det här är inte ett exempel på de kompositioner vi såg i föreläsning två, utan ett exempel på surjektioner.

Vår sats säger oss att svaret är $3!\{{5 \atop 3}\} = 150$.

Mängdpartitioner

Hur många sätt finns det att fördela n objekt i k stycken olika högar? Här har vi en ny variant på räkneproblem – istället för att vi har objekt som är särskiljbara eller inte så har vi nu osärskiljbara *lådor*.

Teorem 5. *Antag att vi har en mängd X med $|X| = n$. Ett sätt att dela upp denna mängd i k osärskiljbara högar*[3] *kallas för en* mängdpartition *av X i k delar.*

Antalet sådana ges av

$$\left\{ {n \atop k} \right\}.$$

[3] Alltså, för den som vill vara formell, ett sätt att skriva $X = A_1 \cup A_2 \cup \ldots \cup A_k$ där $A_i \cap A_j = \emptyset$ för $i \neq j$, där etiketterna på våra A_i inte spelar roll. Eller så kan man se det som en ekvivalensrelation på X med k delar.

Bevis. Vi bevisar detta genom att räkna antalet surjektioner från X till $[k]$ på två olika sätt.

Beteckna antalet mängdpartitioner av X i k delar med m. Vi kan skapa oss en surjektion från X till $[k]$ genom att först dela upp X i k

delar, och sedan ge etiketter från 1 till k till delarna. Vår surjektion blir då att vi skickar del i till talet $i \in [k]$. Eftersom det finns $k!$ sätt att tilldela etiketterna (etiketteringen är en permutation av längd k från $[k]$) säger oss Multiplikationsprincipen att det måste finnas $k!m$ surjektioner från X till $[k]$.

Men vi vet också av Teorem 3 att antalet surjektioner ges av $k!\{{n \atop k}\}$. Alltså måste $m = \{{n \atop k}\}$, som önskat. □

Den tolvfaldiga vägen

När vi talade om kompositioner fördelade vi alltså osärskiljbara objekt i särskiljbara lådor – och studerade både fallet där lådor fick vara tomma, och när de inte fick det. För surjektioner fördelar vi särskiljbara objekt i särskiljbara lådor, och kräver att varje låda får ett objekt.

Vi börjar ana ett mönster här i hur våra problem kan se ut. Vi kan ha

1. Särskiljbara objekt och särskiljbara lådor
2. Osärskiljbara objekt och särskiljbara lådor
3. Särskiljbara objekt och osärskiljbara lådor
4. Osärskiljbara objekt och osärskiljbara lådor

och vi kan ha olika krav på hur objekten fördelas i lådorna

1. Generell – lådor får vara tomma och får innehålla hur många objekt som helst
2. Surjektiv – varje låda måste innehålla något objekt
3. Injektiv – ingen låda får innehålla mer än ett objekt

så sammanfattningsvis har vi en tabell med tolv stycken tänkbara kombinatorikproblem. Det kommer visa sig att vi i själva verket redan studerat sju av dem.

Under föreläsning två pratade vi om fördelningar av osärskiljbara objekt mellan särskiljbara personer, och gav en formel för deras antal i Proposition 11, men vi gav aldrig ett kort namn åt detta problem. Låt oss kalla en sådan fördelning för en *multi-delmängd* till mängden av personer.

En *multi-mängd* är som en vanlig mängd, fast den får innehålla ett och samma objekt mer än en gång. Så vi betraktar alltså fördelningen av objekt mellan personer som en multi-delmängd genom att tänka att varje person är med i multidelmängden lika många gånger som antalet objekt den fick.

Så låt oss rita denna tabell – problem vi redan studerat är i svart text, problem vi inte sett innan är i grön text. Låt N vara en mängd av n *objekt*, och X vara en mängd av x *lådor*. Vi ser fördelningarna av objekt i lådor som en funktion $f : N \to X$.

	Generellt f	Injektivt f	Surjektivt f
Bägge särskiljbara	Ord ur X av längd n x^n	Permutation ur X av längd n $\frac{x!}{(x-n)!}$	Surjektion från N till X $x!\left\{ {n \atop x} \right\}$
Osärskiljbara objekt	Multi-delmängd av X av storlek n $\binom{n+x-1}{n}$	Delmängd av X av storlek n $\binom{x}{n}$	Kompositioner av n av längd x $\binom{n-1}{n-x}$
Osärskiljbara lådor	Mängdpartition av N i $\leq x$ delar $\sum_{k=1}^{x} \left\{ {n \atop k} \right\}$	Mängdpartition av N i $\leq x$ delar av storlek 1 1 om $n \leq x$, 0 annars	Mängdpartition av N i x delar $\left\{ {n \atop x} \right\}$
Bägge osärskiljbara	Heltalspartition av n i $\leq x$ delar $p_x(n+x)$	Sätt att skriva n som summan av $\leq x$ ettor 1 om $n \leq x$, 0 annars	Heltalspartitioner av n i x delar $p_x(n)$

Låt oss ge argument för varför varje av cellerna i denna tabell faktiskt är vad som påstås.

Raden med bägge särskiljbara är den enklaste att fundera på. Om vi tar ett generellt f räknar vi *alla* funktioner från N till X, utan begränsningar och utan att bekymra oss om särskiljbarhet. Ett annat ord för "funktion från N till X" kan vara "ord ur X av längd n" ifall vi tänker oss $N = [n]$. Att kräva att funktionen är injektiv är samma sak som att kräva att ingen bokstav dyker upp två gånger i ordet, vilket ju var vår definition av en permutation. Om det enda vi kräver är att funktionen är surjektiv är så klart vad vi räknar just surjektioner.

I raden med osärskiljbara objekt så kan vi tänka oss objekten som bollar vi lägger i lådorna. Om vi kan acceptera varje fördelning av bollar – lådor får vara tomma eller innehålla mer än en boll – är ju detta precis vårt scenario med att fördela mynt bland personer, vilket vi just gett namnet multi-delmängder. Om varje låda bara får innehålla noll eller en boll, och vi inte kan se skillnad på bollarna, bestäms varje fördelning av bollar bara av vilka lådor som har en boll och vilka som inte har en – alltså av en delmängd av lådorna, och delmängden måste ha samma storlek som antalet bollar. Kräver vi att varje låda måste få en boll är vi i fallet med kompositioner, som vi definierade kort i slutet av biten om multi-delmängder – vi kan få en sådan genom att först ge varje person ett mynt och sedan fördela ut resten av mynten fritt, så vi härleder lätt den formeln ur formeln för multi-delmängder.

I raden med osärskiljbara lådor får vi i stället tänka oss att objekten är distinkta, men vi lägger dem i högar (och tillåter oss högst x olika högar) istället för i lådor – så vi kan inte se skillnad på olika högar

annat än på deras innehåll. Ett av fallen, där vi kräver en surjektion, har vi just behandlat – att varje av våra x högar måste innehålla ett objekt gör bara att vi begränsar oss till att dela upp våra objekt i exakt x högar, alltså att vi gör en mängdpartition av dem i x delar. Om vi inte kräver att funktionen är surjektiv tillåter vi "tomma högar", vilka ju resulterar i att vi har en uppdelning i ett mindre antal faktiska högar. Så formeln är bara att vi summerar den tidigare formeln över varje möjligt antal högar.

Fallet med injektiva f och osärskiljbara lådor är korkat. Vi vill alltså dela upp våra objekt i högst x stycken högar, men kräver att varje hög har som mest ett objekt. Så om $n \leq x$ är detta möjligt – varje objekt får sin egen hög – annars är det omöjligt. Så det finns alltid noll eller ett sätt att göra detta på.

I sista raden, när både objekten och lådorna är osärskiljbara, får vi tänka oss att vi har identiska bollar som vi lägger i högar. Vi kan varken fråga "vilka bollar ligger i den högen" eller "vilken av högarna är det där", vi kan bara se hur många högar av varje storlek det finns. Så låt oss definiera det räkningsproblem detta motsvarar:

Definition 6. En *heltalspartition* av ett heltal n i k delar är ett sätt att skriva n som summan av k stycken heltal större än noll. Ordningen vi skriver heltalen i i summan spelar ingen roll.

Vi betecknar antalet heltalspartitioner av n i k delar med $p_k(n)$.

Till skillnad från varje annat räkneproblem vi studerat hittills finns det ingen enkel formel för $p_k(n)$ i termer av k och n. Men det betyder inte att vi inte kommer kunna säga intressanta kombinatoriska saker om heltalspartitioner.

Exempel 7. Det finns fem heltalspartitioner av 8 i 4 delar. Dessa är:

$$5+1+1+1=8$$
$$4+2+1+1=8$$
$$3+3+1+1=8$$
$$3+2+2+1=8$$
$$2+2+2+1=8$$

Så i sista raden, när vi kräver att funktionen är surjektiv, alltså att vi har exakt x högar, ges antalet sådana funktioner av $p_x(n)$. Om vi inte kräver att funktionen är surjektiv så räknar vi istället alla heltalspartitioner av n i högst x delar. Antalet sådana ges av $p_x(n+x)$ – tänk att vi ger en etta till varje av de x lådorna, och sedan fördelar resten fritt, för att motivera formeln.

Slutligen är sista radens mellersta cell, när vi kräver att funktionen är injektiv, korkad av ungefär samma skäl som varför cellen ovanför

var det. Vad vi kräver är alltså att ingen hög får ha mer än ett objekt – så vi skall skriva n som summan av högst x stycken ettor! Om $n \leq x$ kan vi göra det på ett enda sätt – vi skriver n som summan av n stycken ettor – annars går det inte.

Stirlingtalen av första sorten

I början av denna föreläsningen introducerade vi Stirlingtalen av *andra* sorten, vilket ju leder en till att fråga vad den första sorten är. Så låt oss introducera ett problem till vilket dem är lösningen:

Definition 8. Antag att n personer skall sitta runt k stycken osärskiljbara runda bord, och varje bord måste ha minst en person som sitter vid det. Då ges antalet sätt att placera personerna runt borden av $\left[{n \atop k}\right]$, *Stirlings cykeltal*. Stirlings cykeltal kallas också för *Stirlingtalen av första sorten*.

Till skillnad från Stirlings partitionstal finns det inte någon enkel formel för cykeltalen. Vi kan däremot bevisa följande resultat:

Teorem 9. *Det gäller, för alla $n \geq 1$, att*

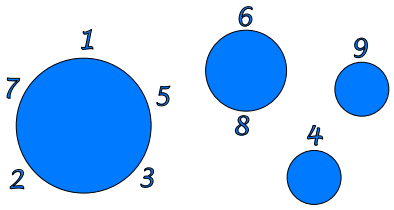
$$\sum_{k=1}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n!.$$

Bevis. Vi bevisar detta genom att uppvisa en bijektion mellan mängden av permutationer av längd n ur $[n]$, vilka vi vet att det finns $n!$ av, och samlingen av sätt att placera personer runt ett godtyckligt antal runda bord, vilka vi vet per definition räknas av $\sum_{k=1}^{n} \left[{n \atop k}\right]$.

Givet ett sätt att placera n personer runt något antal runda bord kan vi definiera en permutation σ genom att, på plats i i permutationen, skriva den person som sitter till vänster om person i runt deras bord. (En person som sitter ensam anser vi sitta till vänster om sig själv.) Detta kommer ge oss en permutation eftersom varje person bara har en person till höger om sig, så ingen person kommer dyka upp två gånger, och varje person har bara en person till vänster om sig, så $\sigma(i)$ är väldefinierat för varje i.

Givet en permutation σ kan vi placera ut personer runt runda bord som följer: Vi börjar med att ställa fram ett bord, och sätta person ett vid det bordet. Sedan sätter vi person $\sigma(1)$ till vänster om person ett, och person $\sigma(\sigma(1))$ till vänster om person $\sigma(1)$, och så vidare. Förr eller senare måste vi komma tillbaka till person 1, eftersom det bara finns ändligt många personer. Om vi placerat alla personerna runt vårt första bord är vi klara.

Om vi har några personer kvar att placera plockar vi fram ett till bord, och sätter den person med lägst nummer som inte redan har en



Figur 1: Ett exempel på ett sätt placera nio personer vid runda bord. Den motsvarande permutationen till detta sätt att placera personer är 572438169. Det vanliga sättet att skriva detta sätt att placera personer vid bord i text är (15327)(4)(68)(9).

sittplats vid det bordet – säg att det är person j. Sedan upprepar vi processen från innan, och placerar person $\sigma(j)$ till vänster om henne, person $\sigma(\sigma(j))$ till vänster om person $\sigma(j)$, och så vidare. Återigen kommer vi förr eller senare komma tillbaka till person k, och ha gått full cirkel.

Vi upprepar denna process med fler bord ända tills varje person har fått ett bord, och vi har fått oss ett sätt att placera n personer runt något antal bord mellan 1 och n.

Det är någorlunda enkelt att se, efter att man funderat en stund, att vi alltid kommer komma tillbaka till samma permutation vi började med om vi först skapar en bordsplacering av permutationen, och sedan skapar en permutation av den bordsplaceringen. Alltså är detta en bijektion, och vi har bevisat vår formel. □

Kommentar 10. Vi har introducerat detta som "personer runt runda bord", men den vanliga matematiska terminologin runt detta är "cykler i en permutation". Hittills har vi bara sett permutationer som en lista av tal i någon ordning, där varje tal mellan 1 och n dyker upp exakt en gång, men detta är bara ett perspektiv på vad en permutation är.

Perspektivet med cykler är ett minst lika vanligt perspektiv på permutationer, och framhäver andra saker man kan använda dem för. För att representera dessa i text skriver vi vanligen i formatet $(15327)(4)(68)(9)$, såsom i Figur 9, i stället för att rita cirklar med tal runt dem.

Övningar

Övning 1. Ge ett kombinatoriskt bevis för följande rekursion för Stirlings partitionstal

$$\left\{ {n \atop k} \right\} = k \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}.$$

Övning 2. Ge kombinatoriska bevis för att

$$\left\{ {n \atop n-1} \right\} = \binom{n}{2}$$

och

$$\left\{ {n \atop 2} \right\} = 2^{n-1} - 1.$$

Övning 3. Ge ett kombinatoriskt bevis för följande rekursion för Stirlings cykeltal

$$\left[{n+1 \atop k} \right] = \left[{n \atop k-1} \right] + n \left[{n \atop k} \right].$$

Övning 4. I slutet av förra föreläsningen talade vi om *derangemang* – alltså permutationer σ sådana att $\sigma(i) \neq i$ för alla i. Om vi i stället tänker på permutationer som sätt att placera personer runt runda bord, hur kan vi se på vår bordsplacering om vår permutation är ett derangemang?

Övning 5. Bevisa att[4]

$$\left\{ {n+1 \atop k+1} \right\} = \sum_{j=k}^{n} \binom{n}{j} \left\{ {j \atop k} \right\}.$$

Övning 6. Skriv följande permutation av $[10]$ i cykelform

$$8, 9, 4, 10, 5, 7, 3, 2, 6, 1.$$

[4] Här ber vi alltså inte specifikt om ett *kombinatoriskt* bevis, även om beviset jag spontant kommer på är sådant. Om ni hittar ett induktionsbevis vore det också intressant.

Ledtråd för det kombinatoriska beviset: Tänk att vi har ett speciellt objekt som är det $n+1$te, och det får hamna i sin speciella del. Så vi väljer hur stor den delen är och sedan fördelar vi ut resten av objekten.

Föreläsning 5: Genererande funktioner · 1MA020

Vilhelm Agdur[1]

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

31 januari 2023

Vi går vidare från våra grundläggande tekniker till en lite mer avancerad metod inom kombinatoriken – genererande funktioner.

Hittills har vi bevisat våra resultat huvudsakligen med hjälp av smarta insikter i strukturen hos problemen – med kombinatoriska argument som ser på samma objekt ur två vinklar, eller ser en bijektion. Det enda större verktyget vi introducerat hittills är inklusion-exklusion.

Det är dags att introducera ett mer systematiskt verktyg som kan användas för många olika problem, och som låter oss använda våra färdigheter i algebra för att uttrycka och lösa kombinatoriska problem.

Genererande funktioner

Definition 1. Antag att vi har en talföljd $a_0, a_1, a_2, \ldots$. Beteckna denna som $\{a_k\}_{k=0}^{\infty}$. Den *genererande funktionen* för denna talföljd ges av

$$F_a(x) = \sum_{k=0}^{\infty} a_k x^k.$$

I den här kursen betraktar vi dessa funktioner som helt och hållet *kombinatoriska* objekt – vi bryr oss inte ett dugg om ifall dessa uttryck faktiskt konvergerar eller inte.[2] Vi bryr oss för det mesta inte ens om att evaluera dem i någon punkt. De är helt och hållet formella objekt som vi bara manipulerar enligt algebrans räkneregler.[3]

[2] Det finns intressanta tillämpningar av att räkna ut konvergensradien för dessa uttryck – det kan säga oss något om hur stort a_k är asymptotiskt, alltså för väldigt stora k. Men det är överkurs för oss.

[3] Det här går att göra rigoröst med en bunt algebra-hokuspokus och termer som "polynomring i oändligt många variabler". Vi skippar det.

Exempel 2. Välj ett fixt heltal n, och låt $a_k = \binom{n}{k}$ för varje k.[4] Den genererande funktionen för denna följd blir då

$$F_a(x) = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

[4] Specifikt blir alltså $a_k = 0$ för $k > n$, eftersom en mängd har noll delmängder större än sig själv.

Om vi använder binomialsatsen kan vi få ett enklare uttryck för denna genererande funktion, eftersom den ger oss att

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} x^k = F_a(x).$$

Exempel 3. Välj ett fixt heltal n, och låt följden a_k ges av att $a_k = 1$ om $k \leq n$ och 0 annars. Dess genererande funktion ges då av

$$\sum_{k=0}^{n} x^k = 1 + x + \ldots + x^n.$$

Vi kan få den på en enklare form genom att observera att

$$\begin{aligned} 1 - x^{n+1} &= (1 + x + x^2 + \ldots + x^n) - (x + x^2 + \ldots + x^{n+1}) \\ &= (1 - x)(1 + x + x^2 + \ldots + x^n) = (1 - x)F_a(x) \end{aligned}$$

och lösa detta uttryck för $F_a(x)$ och få

$$F_a(x) = \frac{1 - x^{n+1}}{1 - x}.$$

Exempel 4. Låt $a_k = 1$ för alla k. Dess genererande funktion är då

$$F_a(x) = \sum_{k=0}^{\infty} x^k$$

vilket vi kan känna igen som en oändlig geometrisk summa, för vilka vi vet att formeln är[5]

$$F_a(x) = \frac{1}{1 - x}.$$

[5] Eller så hade vi kunnat använda samma räkning som i förra exemplet, även om den är lite svårare att rättfärdiga. Eller så känner vi igen det som Taylorserien för $\frac{1}{1-x}$.

Rekursioner

En fråga ni bör ställa er i det här läget är denna: Vad är allt det här bra för? Vi har tagit följder, definierat serier för dem, och hittat uttryck för serierna. Än sen då?

Nyttan med genererande funktioner är till stor del att information från den "kombinatoriska" sidan återspeglas i de genererande funktionerna – så vi kan ta information på ena sidan, manipulera på den sidan, och sedan gå tillbaka till andra sidan och ha lärt oss något nytt. Ofta går vi i riktningen kombinatorik till genererande funktion till kombinatorik, eftersom vi har så mycket mer kunskap om hur man resonerar om funktioner och algebra.

Som ett första exempel på detta, låt oss använda genererande funktioner för att studera rekursioner och rekurrensrelationer.

Exempel 5. Låt oss studera Fibonacciföljden $\{f_k\}_{k=0}^{\infty}$, som ges av att $f_0 = f_1 = 1$ och

$$f_{k+1} = f_k + f_{k-1}$$

för alla $k \geq 1$.

Vad är dess genererande funktion? Vi tar vår rekursion för den och multiplicerar med x^k, och får att

$$f_{k+1}x^k = f_k x^k + f_{k-1}x^k$$

så om vi summerar detta över alla $k \geq 1$ (eftersom dessa är de k för vilka likheten är giltig) får vi att

$$\sum_{k=1}^{\infty} f_{k+1}x^k = \sum_{k=1}^{\infty} f_k x^k + \sum_{k=1}^{\infty} f_{k-1}x^k.$$

Vi ser att alla uttrycken här ser väldigt snarlika ut genererande funktionen för Fibonacciföljden, men ingen av dem är exakt den genererande funktionen. Så om vi manipulerar uttrycken lite får vi att

$$\frac{1}{x}\sum_{k=1}^{\infty} f_{k+1}x^{k+1} = \sum_{k=1}^{\infty} f_k x^k + x\sum_{k=1}^{\infty} f_{k-1}x^{k-1}$$

vilket är ännu närmre. Sista termen är nu precis den genererande funktionen, men de andra startar summan för högt – de skippar de första termerna. Så om vi justerar för detta genom att lägga till noll på ett par ställen får vi att

$$\frac{1}{x}\left(\sum_{k=1}^{\infty} f_{k+1}x^{k+1} + (f_0 - f_0 + f_1 x - f_1 x)\right) = \left(\sum_{k=1}^{\infty} f_k x^k + (f_0 - f_0)\right) + xF_f(x)$$

och nu, när vi flyttar in de extra f_0 och $f_1 x$ vi har köpt oss är uttrycken faktiskt precis den genererande funktionen, och vad vi har är att

$$\frac{1}{x}\Big(F_f(x) - f_0 - f_1 x\Big) = F_f(x) - f_0 + xF_f(x)$$

vilket, om vi kommer ihåg våra initialförutsättningar att $f_0 = f_1 = 1$, blir till att

$$\frac{F_f(x) - x - 1}{x} = F_f(x) - 1 + xF_f(x).$$

Vi har alltså omvandlat det kombinatoriska påståendet om vår rekursion till ett algebraiskt påstående om vår genererande funktion. Och till skillnad från rekursionen kan vi ju enkelt lösa ekvationen för vår genererande funktion och få att

$$F_f(x) = \frac{1}{1 - x^2 - x}.$$

Det här tar oss alltså halvvägs till att ha gjort något intressant – vi har gått från kombinatorik till genererande funktion, och manipulerat den kombinatoriska informationen algebraiskt för att få fram ny information om den genererande funktionen. Men vi är ju intresserade av den kombinatoriska sidan, så vi vill ju översätta den här informationen tillbaka till att säga något intressant om Fibonacciföljden.

En sak man kan göra, men som vi inte skall lägga tid på[6] i denna föreläsningen, är att räkna ut Taylorutvecklingen av denna genererande funktionen, och på så vis få fram en formel för det $n$te Fibonaccitalet.

[6] Vad man får göra är ofta att partialbråksuppdela den genererande funktionen, och att partialbråksuppdela är ju ungefär det tråkigaste man kan göra i matematiken, alltså varför vi skippar att faktiskt göra det.

Ifall man faktiskt genomför den räkningen kommer man att få följande resultat:

Proposition 6 (Binets formel)**.** *Det gäller för Fibonaccitalen att*

$$f_n = \frac{\phi^n - \phi^{-n}}{\phi - \frac{1}{\phi}}$$

där $\phi = \frac{1+\sqrt{5}}{2}$ *är det gyllene snittet.*

Lemma 7 (Räkneregler för genererande funktioner)**.** *Antag att vi har en följd* $\{a_k\}_{k=0}^{\infty}$*, med genererande funktion* F_a*. Då gäller det att*

1. *För varje* $j \geq 1$ *är*

$$\sum_{k=j}^{\infty} a_k x^k = \left(\sum_{k=0}^{\infty} a_k x^k\right) - \left(\sum_{k=0}^{k=j-1} a_k x^k\right) = F_a(x) - \sum_{k=0}^{k=j-1} a_k x^k$$

2. *För alla* $m \geq 0$, $l \geq -m$ *gäller det att*

$$\sum_{k=m}^{\infty} a_k x^{k+l} = x^l \left(\sum_{k=m}^{\infty} a_k x^k\right) = x^l \left(F_a(x) - \sum_{k=0}^{m-1} a_k x^k\right)$$

3. *Det gäller att*[7]

$$\sum_{k=0}^{\infty} k a_k x^k = \frac{F_a'(x)}{x}.$$

[7] Denna räkneregel kan förstås generealiseras till att högre potenser av k motsvarar högre derivator – och om vi istället delar med någon potens av k får vi primitiva funktioner till den genererande funktionen.

Bevis. De första två är tydliga – mellersta uttrycket är närmast ett bevis av påståendet – så vi ger enbart ett bevis av det tredje.

Först observerar vi att $ka_k = 0$ när $k = 0$, så

$$\sum_{k=0}^{\infty} k a_k x^k = \sum_{k=1}^{\infty} k a_k x^k$$

och sedan kommer vi ihåg att $\frac{\mathrm{d}}{\mathrm{d}x} x^k = k x^{k-1}$, vilket ger oss att

$$\begin{aligned}\sum_{k=1}^{\infty} k a_k x^k &= \frac{1}{x} \sum_{k=0}^{\infty} k a_k x^{k-1} \\ &= \frac{1}{x} \sum_{k=1}^{\infty} a_k \frac{\mathrm{d}}{\mathrm{d}x} x^k\end{aligned}$$

och vi minns att derivatan är en linjär operator, så vi kan flytta ut den ur summan och få

$$\begin{aligned}\frac{1}{x} \sum_{k=1}^{\infty} a_k \frac{\mathrm{d}}{\mathrm{d}x} x^k &= \frac{1}{x} \frac{\mathrm{d}}{\mathrm{d}x} \left(\sum_{k=1}^{\infty} a_k x^k\right) \\ &= \frac{1}{x} \frac{\mathrm{d}}{\mathrm{d}x} \left(F_a(x) - a_0\right) = \frac{F_a'(x)}{x}\end{aligned}$$

vilket är vad vi ville bevisa. □

Produkter av genererande funktioner

Nästa sak vi skall diskutera är vad som händer om vi multiplicerar två genererande funktioner – alltså vad det motsvarar på den kombinatoriska sidan.

Definition 8. Låt $\{a_k\}_{k=0}^{\infty}$ och $\{b_k\}_{k=0}^{\infty}$ vara två följder. *Faltningen* av a och b betecknar vi med $a * b$, och $\{(a * b)_k\}_{k=0}^{\infty}$ ges av

$$(a * b)_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Exempel 9. Låt $\{a_k\}_{k=0}^{\infty}$ vara någon följd, och låt $\{b_k\}_{k=0}^{\infty}$ vara följden av bara ettor, alltså $b_k = 1$ för alla k. Vad blir $a * b$?

Enligt definitionen är

$$(a * b)_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_i$$

så följden $a * b$ är helt enkelt $(a_0, a_0 + a_1, a_0 + a_1 + a_2, \ldots)$, alltså de kumulativa summorna av följden.

Exempel 10. Låt $\{a_k\}_{k=0}^{\infty}$ vara någon följd, och låt $\{b_k\}_{k=0}^{\infty}$ vara följden som börjar med n stycken ettor, och sedan är noll. Alltså $b_k = 1$ om $k \leq n$, 0 annars. Vad blir $a * b$?

Enligt definitionen är

$$(a * b)_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=k-n}^{k} a_i$$

så vad vi gör för att räkna ut $(a * b)_k$ är att vi tar summan av de senaste n termerna i a_k.

Låt oss nu berätta vad som händer på den algebraiska sidan när vi faltar på den kombinatoriska sidan.

Teorem 11. *Låt $\{a_k\}_{k=0}^{\infty}$ och $\{b_k\}_{k=0}^{\infty}$ vara två följder med generande funktioner F_a och F_b. Den genererande funktionen för $a * b$ är då $F_a(x)F_b(x)$. Vi har alltså att*

$$F_{a*b}(x) = F_a(x)F_b(x)$$

så generande funktioner omvandlar faltningar till produkter.

Bevis. Vi bevisar detta algebraiskt, genom att helt enkelt skriva upp vad $F_a(x)F_b(x)$ är för något och manipulera uttrycket tills det blir $F_{a*b}(x)$. Så

$$\begin{aligned} F_a(x)F_b(x) &= \left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{l=0}^{\infty} b_l x^l\right) \\ &= \sum_{k,l=0}^{\infty} a_k b_l x^{k+l} \end{aligned}$$

om vi multiplicerar ut de två stora summorna.[8]

[8] Vore det här en kurs i analys hade vi behövt fundera långt och väl på om det faktiskt är tillåtet att multiplicera ut en produkt av oändliga summor på detta viset, och om koefficienterna vi fick verkligen är dessa. Men vi bryr oss inte om vad analytikerna tycker, och bryr oss inte om konvergens – för oss är dessa formella objekt, så de multiplicerar ut enligt de algebraiska regler vi förväntar oss. Vad detta gör med konvergensen är en fråga för någon annan.

Som nästa steg grupperar vi termerna efter exponenten på x, och skriver att

$$\sum_{k,l=0}^{\infty} a_k b_l x^{k+l} = \sum_{j=0}^{\infty} \sum_{\substack{k,l\geq 0 \\ k+l=j}} a_k b_l x^j$$
$$= \sum_{j=0}^{\infty} \left(\sum_{\substack{k,l\geq 0 \\ k+l=j}} a_k b_l \right) x^j.$$

Det här ser ju väldigt mycket ut som en genererande funktion – specifikt en generande funktion för följden $\{c_j\}_{j=0}^{\infty}$ där

$$c_j = \sum_{\substack{k,l\geq 0 \\ k+l=j}} a_k b_l.$$

Men denna kan vi ju skriva på ett lite annat sätt – nämligen

$$\sum_{\substack{k,l\geq 0 \\ k+l=j}} a_k b_l = \sum_{i=0}^{j} a_i b_{j-i}$$

och vi ser att detta är faltningen av a och b, så vi har bevisat resultatet. □

Låt oss formulera detta resultat också för fler än två följder – beviset är det samma men med mer notation, så vi utelämnar det.

Lemma 12. *Antag att $\{a_k^1\}_{k=0}^{\infty}, \{a_k^2\}_{k=0}^{\infty}, \ldots, \{a_k^d\}_{k=0}^{\infty}$ är en samling av d stycken följder. Då gäller det att*[9]

$$(a^1 * a^2 * \ldots * a^d)_k = \sum_{\substack{k_1,k_2,\ldots,k_d\geq 0 \\ k_1+k_2+\ldots+k_d=k}} a_{k_1}^1 a_{k_2}^2 \ldots a_{k_d}^d$$

och

$$F_{a^1 * a^2 * \ldots * a^d}(x) = \prod_{i=1}^{d} F_{a^i}(x).$$

[9] Den uppmärksamma av er, som läst en kurs i algebra, kanske anmärker här på att vi bara definierat $a * b$, så ett uttryck som $a^1 * a^2 * \ldots * a^d$ bara är väldefinierat om faltning är en associativ operation.

Hav förtröstan, frukta icke, faltningen är inte bara associativ utan också kommutativ. Den till och med distribuerar över addition.

Vi tar nu och tillämpar detta maskineri vi byggt upp på ett faktiskt kombinatoriskt problem.

Exempel 13. Låt a_k vara antalet lösningar till

$$x_1 + x_2 + x_3 + x_4 + x_5 = k$$

om vi kräver att alla x_i är ickenegativa heltal. Finn den genererande funktionen till denna följd.

Låt, för $i = 1, 2, \ldots, 5$, a^i vara följden av bara ettor, så $a_k^i = 1$ för alla i och k.

Vi betraktar nu faltningen $a^1 * a^2 * a^3 * a^4 * a^5$. Enligt Lemma 12 är

$$(a^1 * a^2 * a^3 * a^4 * a^5)_k = \sum_{\substack{k_1,k_2,k_3,k_4,k_5 \geq 0 \\ k_1+k_2+k_3+k_4+k_5=k}} a^1_{k_1} a^2_{k_2} a^3_{k_3} a^4_{k_4} a^5_{k_5},$$

men summanden här är ju så klart alltid bara en produkt av fem ettor, alltså ett. Så

$$\begin{aligned}\sum_{\substack{k_1,k_2,k_3,k_4,k_5 \geq 0 \\ k_1+k_2+k_3+k_4+k_5=k}} a^1_{k_1} a^2_{k_2} a^3_{k_3} a^4_{k_4} a^5_{k_5} &= \sum_{\substack{k_1,k_2,k_3,k_4,k_5 \geq 0 \\ k_1+k_2+k_3+k_4+k_5=k}} 1 \\ &= |\{k_1, \ldots, k_5 \geq 0 \mid k_1 + \ldots + k_5 = k\}|\end{aligned}$$

och denna faltningen är alltså precis lika med a, följden vi var ute efter.

Om vi nu tar likheten $a = a^1 * a^2 * \ldots * a^5$ och tar genererande funktionen av bägge sidorna får vi likheten $F_a(x) = F_{a^1 * a^2 * \ldots * a^5}(x)$, och tillämpar vi nu åter Lemma 12 får vi att

$$F_a(x) = F_{a^1}(x) F_{a^2}(x) \ldots F_{a^5}(x) = \left(F_{a^1}(x)\right)^5$$

där vi i sista steget använde att $a^1 = a^2 = \ldots = a^5$, så de alla har samma genererande funktion.

Vi såg i början av föreläsningen att den genererande funktionen för en följd av enbart ettor är $\frac{1}{1-x}$, så vad vi fått ut är att

$$F_a(x) = \left(\frac{1}{1-x}\right)^5.$$

Vi hade så klart gärna haft en explicit formel för antalet lösningar på den här ekvationen. Vi fuskar genom att redan veta vad svaret borde bli, och bevisa att den följden har samma genererande funktion som följden vi just studerade – detta bevisar alltså att följderna är lika med varandra.

Lemma 14. *Fixera något heltal $n \geq 1$, och låt följden $\{a_k\}_{k=0}^{\infty}$ ges av*

$$a_k = \binom{n+k-1}{k}.$$

Den genererande funktionen för denna följden är[10]

$$F_a(x) = \frac{1}{(1-x)^n}.$$

Bevis. Vi bevisar detta med induktion i n. För basfallet $n = 1$ blir $\binom{n+k-1}{k} = \binom{k}{k} = 1$, så följden är konstant ett, och vi vet sedan innan att genererande funktionen för följden av bara ettor är $\frac{1}{1-x}$, så basfallet håller.

[10] Så när vi visat detta exemplet kommer vi alltså att veta att antalet lösningar till

$$x_1 + x_2 + x_3 + x_4 + x_5 = k$$

i ickenegativa heltal är precis

$$\binom{k+4}{k}$$

eftersom vi vet att den genererande funktionen för antalet lösningar till den ekvationen var $\frac{1}{(1-x)^5}$.

I just detta fallet visste vi ju dock redan det tack vare vår formel för antalet multi-delmängder.

För induktionssteget, antag att $n \geq 1$, och vi vill visa att likheten gäller för $n+1$. Vår induktionshypotes är nu att

$$F_a(x) = \sum_{k=0}^{n} \binom{n+k-1}{k} x^k = \frac{1}{(1-x)^n}.$$

Alltså har vi att

$$\frac{\mathrm{d}}{\mathrm{d}x} F_a(x) = \frac{n}{(1-x)^{n+1}},$$

så att

$$\begin{aligned}
\frac{1}{(1-x)^{n+1}} &= \frac{1}{n} \frac{\mathrm{d}}{\mathrm{d}x} F_a(x) \\
&= \frac{1}{n} \frac{\mathrm{d}}{\mathrm{d}x} \left(\sum_{k=0}^{n} \binom{n+k-1}{k} x^k \right) \\
&= \frac{1}{n} \sum_{k=0}^{n} \binom{n+k-1}{k} \frac{\mathrm{d}}{\mathrm{d}x} x^k \\
&= \frac{1}{n} \sum_{k=1}^{n} \binom{n+k-1}{k} k x^{k-1}.
\end{aligned}$$

Notera att vi i sista steget ser att derivatan av x^0 är noll, så termen för $k = 0$ försvinner. Justerar vi summeringsindex lite grann så ser vi att

$$\frac{1}{n} \sum_{k=1}^{n} \binom{n+k-1}{k} k x^{k-1} = \frac{1}{n} \sum_{k=0}^{n} \binom{n+k}{k+1} (k+1) x^k.$$

Så låt oss studera summanden i det här uttrycket. Vi ser att

$$\begin{aligned}
\binom{n+k}{k+1} \frac{k+1}{n} &= \frac{(n+k)!}{(k+1)!(n-1)!} \frac{k+1}{n} \\
&= \frac{(n+k)!}{k!n!} \\
&= \binom{n+k}{k} = \binom{(n+1)+k-1}{k}
\end{aligned}$$

så om vi sätter tillbaka detta i vår summa ser vi att vad vi fått är att

$$\frac{1}{(1-x)^{n+1}} = \sum_{k=0}^{\infty} \binom{(n+1)+k-1}{k} x^k$$

vilket är precis vad vi ville bevisa. □

Övningar

Övning 1. Antag att en följd $\{a_k\}_{k=0}^{\infty}$ lyder en rekurrensrelation

$$a_{k+1} = \sum_{i=0}^{\ell} w_i a_{k-i}$$

för alla $k \geq \ell$, där $(w_0, w_1, w_2, \ldots, w_\ell)$ är en följd med koefficienter.[11]

Använd våra räkneregler i Lemma 7 för att finna ett uttryck för den genererande funktionen F_a.[12]

[11] Om det hjälper kan ni anta att $w_i = 0$ för $i \notin 0, 1, \ldots, \ell$.

[12] Det här är alltså generaliseringen av vad vi gjorde för Fibonnacifölden. Ni kommer finna att ni kan skriva svaret som en rationell funktion med koefficienter som ges av de första termerna i a_k och av vikterna w_i.

Övning 2. Antag att vi har en summa

$$\sum_{k=\ell}^{\infty} \sum_{i=k-\ell}^{k} f(k,i) \tag{1}$$

för någon funktion $f : \mathbb{N}^2 \to \mathbb{R}$. Byt ordningen på summeringen,[13] alltså fyll i frågetecknen i uttrycket

$$\sum_{i=0}^{\infty} \sum_{k=?}^{?} f(?,?)$$

så att det blir lika med vad vi hade i (1).[14]

[13] Det här är väl egentligen bara en övning i att manipulera summor, inte i kombinatorik per se. Men det är användbart att kunna trick som det här för att arbeta med genererande funktioner. Ibland kan "byt ordningen i en summa" till och med vara en bevisteknik i sig.

[14] Tips: För varje par av (k,i), hur många gånger dyker $f(k,i)$ upp i summan i (1)? Det hjälper att rita upp en tabell över par av i och k, och fylla i varje ruta om det paret dyker upp. Om vi har värden på k som rader och värden på i som kolumner räknar (1) "radvis", och när vi byter ordning på summan vill vi i stället räkna "kolumnvis".

Övning 3. Låt, om $\{a_k\}_{k=0}^{\infty}$ och $\{b_k\}_{k=0}^{\infty}$ är två följder, $a+b$ vara följden som ges av $(a+b)_k = a_k + b_k$. Bevisa att $F_{a+b}(x) = F_a(x) + F_b(x)$, så att addition på den kombinatoriska sidan motsvarar addition också på den algebraiska sidan.

Bevisa sedan, om $\{c_k\}_{k=0}^{\infty}$ är en tredje följd, att

$$a * (b+c) = a * b + a * c,$$

det vill säga att faltning distribuerar över addition.[15]

[15] Ledtråd: Använd genererande funktioner, specifikt vad ni bevisade i första halvan av uppgiften och Teorem 11.

Övning 4. Låt f_k vara följden av Fibonaccital, såsom vi definierat dem. Låt följden g_k vara $(1,-1,-1,0,0,0,\ldots)$.

1. Vad är den genererande funktionen för $\{g_k\}_{k=0}^{\infty}$?
2. Vad är faltningen $f * g$? Räkna ut detta som om ni inte visste vad den genererande funktionen till f är, alltså utan att använda er av Teorem 11.
3. Använd vad ni gjorde i de första två delfrågorna och Teorem 11 för att ge ett alternativt bevis för att

$$F_f(x) = \frac{1}{1-x-x^2}.$$

Övning 5. Använd genererande funktioner[16] för att bevisa att

$$\sum_{i=0}^{k} (-1)^i \binom{n}{i} \binom{n+k-i-1}{k-i} = 0$$

för alla $k \geq 1$.[17]

[16] Ledtråd: Betrakta den här summan som en faltning av två följder – en av dem kan vi redan den genererande funktionen för, den andra är enkel att finna den genererande funktionen för givet vad vi redan kan. Använd sedan Teorem 11 för att få ut likheten.

[17] Frivillig bonus om ni har tråkigt någon dag: Kan ni komma på ett kombinatoriskt bevis för den här likheten? Jag funderade på det en kort stund och fann inget.

Övning 6. Finn enkla uttryck för de genererande funktionerna för följderna

$$a_k = 3^k, \qquad b_k = \left(\frac{1}{4}\right)^k$$

och

$$c_k = \frac{5}{k!}.$$

Föreläsning 6: Fortsättning på genererande funktioner · 1MA020

Vilhelm Agdur[1]

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

7 februari 2023

Vi fortsätter förra föreläsningens diskussion om genererande funktioner, och använder dem för att räkna lösningar till ekvationer. Sedan introducerar vi exponentiella genererande funktioner, och använder dessa för att lösa några problem.

Antal lösningar till en ekvation, med begränsningar

I slutet på förra föreläsningen studerade vi antalet lösningar till ekvationen

$$x_1 + x_2 + x_3 + x_4 + x_5 = k$$

om vi kräver att alla x_i är ickenegativa heltal. Det var ett första exempel på en mer generell kategori av problem med att räkna lösningar på ekvationer. Låt oss börja med ett lite mer invecklat problem:

Exempel 1. Hur många lösningar finns det till

$$x_1 + x_2 + x_3 + x_4 = k$$

om vi kräver att alla x_i är ickenegativa heltal, men också kräver att x_2 är jämnt, att $x_3 \leq 10$, och x_4 är udda?

Låt, för varje k, a_k vara antalet sådana lösningar. Låt sedan a_k^1 vara antalet lösningar till $x_1 = k$ i ickenegativa heltal x_1, a_k^2 vara antalet lösningar till $x_2 = k$ i ickenegativa jämna heltal, a_k^3 vara antalet lösningar till $x_3 = k$ i heltal mellan 0 och 10, och a_k^4 vara antalet lösningar till $x_4 = k$ i udda heltal.

Precis som i förra exemplet studerar vi nu faltningen av dessa fyra följder, och ser att

$$(a^1 * a^2 * a^3 * a^4)_k = \sum_{\substack{k_1,k_2,k_3,k_4 \geq 0 \\ k_1+k_2+k_3+k_4=k}} a_{k_1}^1 a_{k_2}^2 a_{k_3}^3 a_{k_4}^4 = a_k$$

eftersom $a_{k_1}^1 a_{k_2}^2 a_{k_3}^3 a_{k_4}^4$ är en produkt av ettor och nollor – att $k_1 + k_2 + k_3 + k_4 = k$ garanteras av definitionen av faltning, och sedan är varje term i produkten ett om värdet på k_i är tillåtet av våra begränsningar, och noll annars. Så produkten är ett om summan är korrekt och varje enskild begränsning är uppfylld.

Så precis som i förra exemplet kan vi få fram genererande funktionen för a_k, följden vi faktiskt är intresserade av, genom att plocka fram den genererande funktionen för de enklare följderna.

Vad genererande funktionen för a^1 är vet vi sedan innan – den är bara en följd av ettor, så dess genererande funktion blir $\frac{1}{1-x}$. Likaledes vet vi sedan innan att följden av n stycken ettor och sedan nollor har genererande funktion $\frac{1-x^{n+1}}{1-x}$, så genererande funktionen för a^3 blir $\frac{1-x^{11}}{1-x}$.

Däremot för a^2 behöver vi räkna ut något nytt, nämligen den genererande funktionen för följden $1, 0, 1, 0, 1, \ldots$, indikatorfunktionen av de jämna talen. Så vi får skriva att

$$\begin{aligned} F_{a^2}(x) &= \sum_{k=0}^{\infty} a_k^2 x^k \\ &= \sum_{\substack{k\geq 0 \\ k\in 2\mathbb{Z}}} x^k \\ &= \sum_{i=0}^{\infty} x^{2i} \\ &= \sum_{i=0}^{\infty} (x^2)^i \end{aligned}$$

och sista raden här kan vi känna igen som genererande funktionen av följden $(1, 1, 1, 1, \ldots)$, *utvärderad i* x^2. Så detta är lika med $\frac{1}{1-x^2}$.

Så vad som återstår är alltså a^4, indikatorfunktionen för de udda talen. För att få fram dess genererande funktion kan vi använda vad vi just gjorde för de jämna talen:

$$\begin{aligned} F_{a^4}(x) &= \sum_{k=0}^{\infty} a_k x^k \\ &= \sum_{\substack{k\geq 1 \\ k \text{ udda}}} x^k \\ &= x \sum_{\substack{k\geq 1 \\ k \text{ udda}}} x^{k-1} \\ &= x \sum_{\substack{k\geq 0 \\ k\in 2\mathbb{Z}}} x^k \\ &= \frac{x}{1-x^2}. \end{aligned}$$

Så, om vi använder att genererande produkten av en faltning är produkten av de genererande funktionerna, ser vi att

$$\begin{aligned} F_a(x) &= \left(\frac{1}{1-x}\right)\left(\frac{1-x^{11}}{1-x}\right)\left(\frac{1}{1-x^2}\right)\left(\frac{x}{1-x^2}\right) \\ &= \frac{x(1-x^{11})}{(1-x)^2(1-x^2)^2} \end{aligned}$$

och ber vi vårt favorit-CAS[2] att Taylorutvidga detta uttryck så får vi att

$$F_a(x) = x + 2x^2 + 5x^3 + 8x^4 + 14x^5 + 20x^6 + 30x^7 + 40x^8 + \ldots$$

[2] *Computer Algebra System*, alltså till exempel *WolframAlpha* eller något av dess öppna alternativ, såsom *Sage*.

så att följden av antalet lösningar är

$$0, 1, 2, 5, 8, 14, 20, 30, 40, 55, 70, 91, 111, 138, 163, \ldots.$$

Exempel 2. Vi vill räkna antalet lösningar a_k till ekvationen

$$2x_1 + x_2 + x_3 = k$$

där alla x_i är heltal, x_2 är en multipel av 6, och talet x_3 kan vara antingen rött eller blått.[3]

Vi börjar med att göra variabelbytet $y_1 = 2x_1$, och vill alltså nu ha lösningar till $y_1 + x_2 + x_3 = k$, med begränsningen att y_1 är jämnt. Det här förändrar så klart inte antalet lösningar, bara gör det lättare för oss att tillämpa vår metod.

Vi tillämpar samma metod som i förra exemplet, och låter a_k^1 vara antalet lösningar till $y_1 = k$ med y_1 jämnt, a_k^2 vara antalet lösningar till $x_2 = k$ med x_2 delbart med 6, och a_k^3 vara antalet lösningar till $x_3 = k$ med x_3 färgat antingen rött eller blått. Faltningen blir då

$$(a^1 * a^2 * a^3)_k = \sum_{\substack{k_1,k_2,k_3 \geq 0 \\ k_1+k_2+k_3=k}} a_{k_1}^1 a_{k_2}^2 a_{k_3}^3 = a_k.$$

Vi fortsätter precis som innan med att räkna ut den genererande funktionen för varje av våra följder. För a^1 vet vi redan vad genererande funktionen för indikatorfunktionen av de jämna talen är, nämligen $\frac{1}{1-x^2}$.

För a^2 kan vi använda samma metod som vi använde för de jämna talen för att se att

$$\begin{aligned} F_{a^2}(x) &= \sum_{k=0}^{\infty} a_k^2 x^k = \sum_{\substack{k \geq 0 \\ k \in 6\mathbb{Z}}} x^k \\ &= \sum_{i=0}^{\infty} x^{6i} = \sum_{i=0}^{\infty} (x^6)^i \end{aligned}$$

så att $F_{a^2}(x) = \frac{1}{1-x^6}$.

För a^3 så blir denna helt enkelt en följd av bara tvåor, eftersom vi har två val för färg för varje tal, och kan välja vilket tal som helst. Så vi ser att

$$F_{a^3}(x) = \sum_{k=0}^{\infty} 2x^k = 2\frac{1}{1-x}.$$

Sammantaget har vi alltså att

$$F_a(x) = \left(\frac{1}{1-x^2}\right)\left(\frac{1}{1-x^6}\right)\left(\frac{2}{1-x}\right) = \frac{2}{(1-x)(1-x^2)(1-x^6)}$$

vilket vi kan Taylorutvidga i vårt favoritprogram och få att[4]

$$\begin{aligned} F_a(x) = 2 &+ 2x + 4x^2 + 4x^3 + 6x^4 + 6x^5 + 10x^6 + 10x^7 \\ &+ 14x^8 + 14x^9 + 18x^{10} + 18x^{11} + 24x^{12} + 24x^{13} \\ &+ 30x^{14} + 30x^{15} + 36x^{16} + 36x^{17} + 44x^{18} + \ldots. \end{aligned}$$

[3] Vi ser alltså, för $k = 6$, alla dessa som godtagbara distinkta lösningar:

$x_1 = 1, x_2 = 0, x_3 = 4$, $x_1 = 1, x_2 = 0, x_3 = 4$,

$x_1 = 2, x_2 = 0, x_3 = 2$, $x_1 = 0, x_2 = 6, x_3 = 0$.

[4] Vi ser ju ett tydligt mönster här av att $a_{2k} = a_{2k+1}$. Kan du förklara varför detta måste vara fallet, baserat på våra begränsningar av variablerna?

Att omvandla ett problem till en rekursion

Vårt nästa exempel handlar inte om att räkna lösningar till en ekvation, utan om att översätta ett problem till en rekursion. Vi tar detta exemplet nu delvis eftersom vi kommer vilja ha en rekursion att lösa i ett senare exempel.

Exempel 3. Antag att vi har ett schackbräde med $2 \times n$ rutor, och vi vill täcka det med brickor av formen 2×1 eller 1×2. Hur många sätt kan vi göra detta på?

Låt t_n vara antalet sätt vi kan täcka vårt schackbräde. Vi vill hitta en rekursion för detta antal. Vi ser enkelt att det finns ett enda sätt att göra det för $n = 1$ – bara en bricka får plats – så $t_1 = 1$. För $n = 2$ finns det två sätt, antingen lägger vi dem horisontellt eller vertikalt, så $t_2 = 2$.

Om vi vill skapa oss en täckning av en $2 \times n$-bräda, för något $n > 2$, kan vi göra på två sätt:

- Vi börjar med en täckning av en $2 \times (n-1)$-bräda, och lägger till en till bricka vertikalt.
- Vi börjar med en täckning av en $2 \times (n-2)$-bräda, och lägger till två till brickor horisontellt.

Att varje täckning av en $2 \times n$-bräda kan skapas på detta vis är enkelt att se – antingen är den sista kolumnen täckt av en vertikal bricka, i vilket fall vi skapade täckningen på första viset, eller så är den täckt av två horisontella brickor, i vilket fall vi skapade den på det andra sättet.

Alltså har vi funnit följande rekursion för antalet täckningar

$$t_0 = 0, t_1 = 1, t_2 = 2, \quad t_n = t_{n-1} + t_{n-2} \, \forall n > 2$$

som ju är extremt lik den vi har för Fibonaccitalen, så vi kan finna en genererande funktion och sluten form på precis samma vis som i det fallet.

Figur 1: Ett sätt att göra detta då $n = 8$. Figur tagen ur förra årets anteckningar.

Figur 2: De två sätten att göra det på då $n = 2$. Figur från förra årets föreläsningsanteckningar.

Exponentiella genererande funktioner

Ibland får vi problem med att hitta enkla uttryck för våra genererande funktioner, eftersom vår följd växer för snabbt. Hittills har vi bara studerat följder som växer långsamt nog, men om vi till exempel hade velat studera följden $0!, 1!, 2!, \ldots$ hade dess vanliga genererande funktion varit

$$\sum_{k=0}^{\infty} k! x^k$$

för vilken det inte finns något enkelt uttryck.[5]

[5] Om vi sätter på oss våra analytiker-glasögon kan vi dessutom se att detta uttryck inte konvergerar för något $x > 0$, så vad hade vi ens kunna ha för uttryck för en funktion som är oändlig överallt?

Ett annat exempel på detta är om vi räknar permutationer – dessa kommer vara ungefär $k!$ stycken, i de flesta av våra exempel. Så vi hade haft samma problem. Det finns en anledning att vi hittills bara studerat binomialkoefficienter, som ju är betydligt mindre.

Så, låt oss definiera en variant på genererande funktioner som kan hantera dessa snabbväxande följder.

Definition 4. Om $\{a_k\}_{k=0}^{\infty}$ är någon följd ges dess *exponentiella genererande funktion* av[6]

$$EG_a(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!}.$$

[6] Om vi behöver förtydliga skillnaden kallar vi de icke-exponentiella genererande funktionerna vi studerade innan för *ordinära* genererande funktioner.

Så allt vi faktiskt har gjort är att skala ner vår följd så att den inte växer så kraftigt. Som tur är fungerar detta enkla trick väldigt väl – låt oss räkna några exempel för att se hur.

Exempel 5. Den exponentiella genererande funktionen för följden $(1, 1, 1, 1, \ldots)$ ges av

$$\sum_{k=0}^{\infty} \frac{x^k}{k!} = e^x.$$

Exempel 6. Den exponentiella genererande funktionen för följden $(0!, 1!, 2!, 3!, \ldots)$ ges av

$$\sum_{k=0}^{\infty} k! \frac{x^k}{k!} = \sum_{k=0}^{\infty} x^k = \frac{1}{1-x}.$$

Exempel 7. Fixera något heltal n, och låt a_k vara antalet permutationer av längd k ur ett alfabete med n bokstäver, så att $a_k = \frac{n!}{(n-k)!}$. Då ges den exponentiella genererande funktionen för a av

$$\begin{aligned} EG_a(x) &= \sum_{k=0}^{\infty} \frac{n!}{(n-k)!} \frac{x^k}{k!} \\ &= \sum_{k=0}^{\infty} \frac{n!}{k!(n-k)!} x^k \\ &= \sum_{k=0}^{\infty} \binom{n}{k} x^k = (1+x)^n \end{aligned}$$

där vi i sista ledet kände igen en *ordinär* genererande funktion för binomialkoefficienterna.

Exempel 8. Låt oss återvända till exemplet med schackbrädena. Vi hade en följd som gavs av rekursionen[7]

$$t_0 = 0, t_1 = 1, t_2 = 2, \quad t_{k+2} = t_{k+1} + t_k \; \forall k \geq 1.$$

[7] Notera att vi har ändrat om i rekursionen så att vi har plustecken i index istället för minus – det är fortfarande precis samma rekursion, men vi får finare uttryck senare.

Vad är den exponentiella genererande funktionen för denna följden? Analogt med det ordinära fallet tar vi vår rekursion, multiplicerar den med $\frac{x^k}{k!}$, och summerar över alla $k \geq 1$, för att få att

$$\sum_{k=1}^{\infty} t_{k+2} \frac{x^k}{k!} = \sum_{k=1}^{\infty} t_{k+1} \frac{x^k}{k!} + \sum_{k=1}^{\infty} t_k \frac{x^k}{k!}.$$

Nu kan vi komma ihåg att

$$\frac{\mathrm{d}}{\mathrm{d}x}\frac{x^k}{k!} = \frac{x^{k-1}}{(k-1)!}$$

så att

$$t_{k+1}\frac{x^k}{k!} = t_{k+1}\left(\frac{\mathrm{d}}{\mathrm{d}x}\frac{x^{k+1}}{(k+1)!}\right)$$

och

$$t_{k+2}\frac{x^k}{k!} = t_{k+2}\left(\frac{\mathrm{d}^2}{\mathrm{d}x^2}\frac{x^{k+2}}{(k+2)!}\right).$$

Om vi använder dessa likheter i vad vi hade innan, och bryter ut derivatorna ur summorna, får vi alltså att

$$\frac{\mathrm{d}^2}{\mathrm{d}x^2}\left(\sum_{k=1}^{\infty} t_{k+2}\frac{x^{k+2}}{(k+2)!}\right) = \frac{\mathrm{d}}{\mathrm{d}x}\left(\sum_{k=1}^{\infty} t_{k+1}\frac{x^{k+1}}{(k+1)!}\right) + \left(\sum_{k=1}^{\infty} t_k\frac{x^k}{k!}\right).$$

Precis som i vårt exempel med Fibonaccitalen ser vi nu att vi nästan har de exponentiella genererande funktionerna, förutom att det saknas några av de första termerna i summorna. Så om vi justerar för detta får vi att

$$\begin{aligned}\frac{\mathrm{d}^2}{\mathrm{d}x^2}&\left(EG_t(x) - t_0\frac{x^0}{0!} - t_1\frac{x^1}{1!} - t_2\frac{x^2}{2!}\right) = \\ &= \frac{\mathrm{d}}{\mathrm{d}x}\left(EG_t(x) - t_0\frac{x^0}{0!} - t_1\frac{x^1}{1!}\right) + \left(EG_t(x) - t_0\frac{x^0}{0!}\right)\end{aligned}$$

så om vi substituerar in $t_0 = 0, t_1 = 1, t_2 = 2$ och flyttar in derivatorna i parenteserna så får vi att

$$EG_t''(x) - 2 = EG_t'(x) - 1 + EG_t(x)$$

vilket ju är en helt vanlig andra gradens linjär ordinär differentialekvation med konstanta koefficienter. Randvillkoren för den ges av $EG_t(0) = t_0$ och $EG_t'(0) = t_1$.[8]

Så vi kan antingen lösa den för hand eller med hjälp av vårt favorit-CAS, och finna lösningen

$$\frac{1}{10}\left(\sqrt{5}e^{\left(\frac{\sqrt{5}}{2}+\frac{1}{2}\right)x} - \sqrt{5}e^{\left(\frac{1}{2}-\frac{\sqrt{5}}{2}\right)x} + 5e^{\left(\frac{\sqrt{5}}{2}+\frac{1}{2}\right)x} + 5e^{\left(\frac{1}{2}-\frac{\sqrt{5}}{2}\right)x} - 10\right)$$

vilket vår CAS[9] låter oss se kan Taylorutvidgas till

$$\sum_{n=1}^{\infty}\frac{\left(5-\sqrt{5}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n + \left(5+\sqrt{5}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n}{10}\frac{x^n}{n!}$$

vilket alltså ger oss en direkt formel för varje term i följden, i samma still som för Fibonaccitalen.

[8] Detta kommer ju alltid gälla för alla exponentiella genererande funktioner, av hur de är definierade.

[9] Eller vi, för hand, om vi inte är lata. Den enda funktionen som är involverad är ju e^x, så det är inget svårt att expandera, bara många termer att hålla ordning på.

Vad vi sett i detta exemplet är alltså att vi, när vi har en felmatchning mellan index i vår följd och index i $\frac{x^k}{k!}$, plockar på oss derivator – till skillnad från i fallet med ordinära genererande funktioner, då detta gav oss faktorer av x.

Vi har också sett att de exponentiella genererande funktioner vi hittar för linjära rekursioner kommer ha en bunt olika e^{Cx} för konstanter C,[10] vilket är mycket enklare att Taylorutvidga. Så om man vill lösa linjära rekursioner i praktiken är exponentiella genererande funktioner ofta ett bättre val än ordinära.

[10] Precis som vi såg för följden $(1, 1, 1, \ldots)$, där $C = 1$ – detta beror, i alla fall andligen, på att våra följder som ges av linjära rekursioner också kommer växa ungefär så långsamt, så vi får samma sorts funktion.

Binomial-faltningar och EGFer

Vi har lärt oss att motsvarigheten till en faltning på den kombinatoriska sidan är en produkt av genererande funktioner. Vad händer om vi i stället tar *exponentiella* genererande funktioner? Situationen blir lite mer komplicerad.[11]

[11] Det verkar som att både kursboken och förra årets föreläsningsanteckningar sveper denna komplikation under mattan, på ett sätt som jag upplever som väldigt förvirrande. Det tog mig minst en timme att lista ut varför vad de gör inte är direkt felaktigt.

Definition 9. Antag att $\{a_k\}_{k=0}^{\infty}$ och $\{b_k\}_{k=0}^{\infty}$ är två följder. Då ges deras *binomial-faltning* $a \circledast b$ av

$$(a \circledast b)_k = \sum_{i=0}^{k} \binom{k}{i} a_i b_{k_i}.$$

Lemma 10. *Antag att $\{a_k\}_{k=0}^{\infty}$ och $\{b_k\}_{k=0}^{\infty}$ är två följder, vars exponentiella genererande funktioner är $EG_a(x)$ och $EG_b(x)$. Då ges den genererande funktionen för binomial-faltningen $a \circledast b$ av*

$$EG_{a \circledast b}(x) = EG_a(x) EG_b(x)$$

Bevis. Lägg märke till att EG_a inte bara är den exponentiella genererande funktionen för a, utan också är den ordinära genererande funktionen för $A_k = \frac{a_k}{k!}$, och likaledes för b. Alltså måste, enligt vad vi redan vet om ordinära genererande funktioner,

$$EG_a(x) EG_b(x) = G_A(x) G_B(x) = G_{A * B}(x).$$

Så vad vi studerar är den vanliga faltningen av A med B – vi ser att denna är

$$\begin{aligned}
(A * B)_k &= \sum_{i=0}^{k} A_i B_{k-i} \\
&= \sum_{i=0}^{k} \frac{a_i}{i!} \frac{b_{k-i}}{(k-i)!} \\
&= \sum_{i=0}^{k} \frac{k!}{i!(k-i)!} \frac{a_i b_{k-i}}{k!} \\
&= \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i} \frac{1}{k!} = (a \circledast b)_k \frac{1}{k!}
\end{aligned}$$

så alltså måste vi ha

$$\begin{aligned} G_{A*B}(x) &= \sum_{k=0}^{\infty} (A * B)_k x^k \\ &= \sum_{k=0}^{\infty} (a \circledast b)_k \frac{x^k}{k!} \\ &= EG_{a \circledast b}(x) \end{aligned}$$

och vårt lemma är bevisat. □

På ett fullkomligt analogt sätt, användandes resultatet för ordinära genererande funktioner, fast med fler index, kan vi bevisa följande resultat:

Lemma 11. *Antag att* $\{a_k^1\}_{k=0}^{\infty}, \{a_k^2\}_{k=0}^{\infty}, \ldots, \{a_k^d\}_{k=0}^{\infty}$ *är följder. Då gäller det att*[12]

$$(a^1 \circledast a^2 \circledast \ldots \circledast a^d)_k = \sum_{\substack{k_1,k_2,\ldots,k_d \\ k_1+k_2+\ldots+k_d=k}} \left(\binom{k}{k_1, k_2, \ldots, k_d} \prod_{j=1}^{d} a_{k_j}^j \right)$$

och

$$EG_{a^1 \circledast a^2 \circledast \ldots \circledast a^d}(x) = \prod_{j=1}^{d} EG_{a^j}(x).$$

[12] Kom ihåg att notationen $\binom{k}{k_1,k_2,\ldots,k_d}$ betecknar en *multinomialkoefficient*.

Som vårt sista exempel för denna föreläsning tar vi motsvarigheten för exponentiella genererande funktioner till våra problem med antal lösningar på en ekvation.

Exempel 12. Hur många strängar ur alfabetet $\{a, b, c, d\}$ finns det av längd k, med åtminstone ett b, högst tre c, och ett jämnt antal d?

Precis som i fallet med att räkna lösningar till ekvationer låter vi l_k vara antalet sådana strängar, och låter sedan

- a_k vara antalet strängar ur alfabetet $\{a\}$ av längd k,
- b_k vara antalet strängar ur alfabetet $\{b\}$ av längd k med åtminstone ett b,
- c_k vara antalet strängar ur alfabetet $\{c\}$ av längd k med högst tre c, och
- d_k vara antalet strängar ur alfabetet $\{d\}$ av längd k med ett jämnt antal d.

Om vi nu betraktar binomialfaltningen av dessa fyra följder ser vi att

$$(a \circledast b \circledast c \circledast d)_k = \sum_{\substack{k_1,k_2,k_3,k_4 \\ k_1+k_2+k_3+k_4=k}} \binom{k}{k_1, k_2, k_3, k_4} a_{k_1} b_{k_2} c_{k_3} d_{k_4} = l_k$$

eftersom vad vi räknar med multinomialkoefficienten $\binom{k}{k_1,k_2,k_3,k_4}$ är precis antalet strängar av längd k med k_1 stycken a, k_2 stycken b, och så vidare.

Vad som återstår är alltså att finna de exponentiella genererande funktionerna för våra fyra följder.

- Följden a är helt enkelt $(1,1,1,\ldots)$, så dess exponentiella genererande funktion har vi redan sett är e^x.
- Följden b är $(0,1,1,\ldots)$, så vi kan räkna att

$$EG_b(x) = \sum_{k=1}^{\infty} \frac{x^k}{k!} = \sum_{k=0}^{\infty} \frac{x^k}{k!} - 1 = e^x - 1.$$

- Följden c är $(1,1,1,1,0,0,\ldots)$, så

$$EG_c(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{6}.$$

- För följden d får vi använda oss av ett litet trick, och skriva att

$$\begin{aligned} EG_d(x) &= \sum_{k \in 2\mathbb{Z}^{\geq 0}} \frac{x^k}{k!} \\ &= \frac{1}{2}\left(\sum_{k=0}^{\infty} \frac{x^k}{k!} - \sum_{k=0}^{\infty} \frac{(-x)^k}{k!}\right) \\ &= \frac{e^x - e^{-x}}{2}. \end{aligned}$$

Multiplicerar vi ihop dessa får vi att

$$EG_l(x) = e^x\left(e^x - 1\right)\left(1 + x + \frac{x^2}{2} + \frac{x^3}{3}\right)\left(\frac{e^x - e^{-x}}{2}\right).$$

Om vi vill ha en explicit formel är ett bra nog CAS[13] kapabelt att ge en explicit formel för den $n$te termen i serieexpansionen av detta, men den är inte vacker.

[13] Mathematica kan det, men inte WolframAlpha.

Övningar

Övning 1. Hur många heltalslösningar till ekvationen

$$x_1 + x_2 + x_3 = 578$$

finns det,[14] om vi kräver att

- $x_1 \geq -7$,[15]
- $x_2 \geq 0$ är ett jämnt tal,

[14] Om ni väl har hittat genererande funktionen för antalet lösningar när vi ersatt 578 med k, så kan ni enkelt få fram svaret med följande kod till *WolframAlpha*:

`SeriesCoefficient`$[f, \{x, 0, 578\}]$

där f då är genererande funktionen ni funnit. Att ange den genererande funktionen och säga att ni sedan plockade fram rätt koefficient ur den med hjälp av ett CAS är den förväntade metoden här.

[15] Ledtråd: Gör ett variabelbyte till y_1 för att få den vanliga begränsningen att $y_1 \geq 0$.

- och $x_3 \geq 0$ kan vara vilket tal som helst, men om det är jämnt kan det vara rött eller blått, och om det är udda kan det vara gult, grönt, eller lila.

Övning 2. Antag att vi vet att följden $\{a_k\}_{k=0}^{\infty}$ har exponentiell genererande funktion F. Finn ett enkelt uttryck för den exponentiella genererande funktionen för följden $b_k = ka_k$, i termer av F.

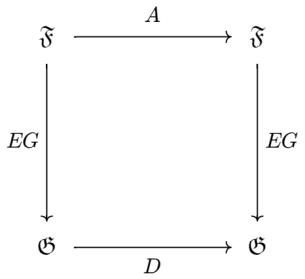
Övning 3. I denna övning använder vi ett lite mer abstrakt språk. Låt $\mathfrak{F}$ vara mängden av alla följder, och $\mathfrak{G}$ vara mängden av alla genererande funktioner. Då kan vi alltså låta $G : \mathfrak{F} \to \mathfrak{G}$ vara funktionen som skickar en följd till dess ordinära genererande funktion, och $EG : \mathfrak{F} \to \mathfrak{G}$ funktionen som skickar en följd till dess exponentiella genererande funktion.

Vi kan också definiera operatorn (funktionen) $A : \mathfrak{F} \to \mathfrak{F}$ som att $(Aa)_k = a_{k+1}$. Vi förskjuter alltså index ett steg, och slänger bort första termen i vår följd.[16] Likaledes kan vi definiera operatorn $D : \mathfrak{G} \to \mathfrak{G}$ som funktionen som skickar en genererande funktion på dess derivata.[17]

Slutligen kan vi, för varje heltal n, definiera operatorn $T_n : \mathfrak{F} \to \mathbb{R}$ som att $Ta = a_n$. Den plockar alltså helt enkelt ut den $n$te termen i följden.

Låt oss nu plocka ner all denna abstraktionen på en lite mer konkret nivå. Övertyga er själva, genom att skriva ut konkret vad påståendena betyder, om att vi redan visat i föreläsningarna att

- $G(A(a)) = \frac{1}{x}\left(G(a) - T_0(a)\right)$ och
- $EG(A(a)) = D(EG(a))$. Vill man vara oerhört förfinad och abstrakt kan man formulera detta som att följande diagram kommuterar:



Övning 4. Låt oss nu se varför detta abstrakta språk faktiskt är användbart ibland.[18] Låt $a = (1,0,0,1,0,0,1,\ldots)$, och låt $\overrightarrow{1} = (1,1,1,\ldots)$.

Visa att

$$a = \overrightarrow{1} - Aa - AAa,$$

[16] Så till exempel har vi att $A(1,0,1,0,1,0,\ldots) = (0,1,0,1,0,1,\ldots)$.

[17] Vi har ju egentligen inte *definierat* vad vi menar med derivatan av en genererande funktion, utan bara låtsats att vi får behandla dem som vilken funktion som helst, och ignorerat alla konvergensfrågor och allt krångel om att summorna har oändligt med termer. Vi fortsätter att göra så.

[18] I det här fallet ger det oss ett mycket koncisare sätt att uttrycka räkningen för att hitta genererande funktionen för indikatorföljden för talen delbara med tre. Dessutom blir det tydligt hur man hade gjort om vi hade sju istället för tre.

Kanske att man till och med kan göra räkningen för godtyckliga $n\mathbb{Z}$, men det kräver nog mer differentialekvationsteori än jag kan, eller kan förvänta mig att ni skall kunna. (Jag försökte i ungefär en minut med Laplacetransformer, men det blev svårt och kändes invecklat.)

använd vad vi just gjorde i förra övningen för att omvandla detta till en differentialekvation för $EG(a)$, och lös differentialekvationen[19] för att få fram ett uttryck för exponentiella genererande funktionen för a.

[19] Det här steget vill jag inte ha några räkningar på – bara ange vad lösningen blir. Ni får använda vilket verktyg ni vill för att faktiskt lösa den.

Övning 5. Låt ℓ_k vara antalet strängar ur alfabetet $\{a, b, c\}$ av längd k, sådana att

- det omedelbart efter varje a följer ett b,[20]
- det finns ett jämnt antal c,
- antalet a är delbart med tre,
- och varje b föregås av ett a?

Finn genererande funktionen för följden ℓ_k.

[20] Ledtråd: För att hantera denna begränsning behöver vi göra ett "variabelbyte". Vad kan det tänkas betyda i denna kontext?

Övning 6. För varje n ges det $n$te *Bell-talet* av

$$B_n = \sum_{k=1}^{n} \left\{ n \atop k \right\},$$

så det räknar alltså det totala antalet mängdpartitioner av en mängd av n element, oavsett antal delar. Man kan visa att[21]

[21] Detta är en av övningarna i vår samling med extra övningar.

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k. \tag{1}$$

Låt $EG_B(x)$ vara den exponentiella genererande funktionen för Bell-talen, och visa att

$$\frac{\mathrm{d}}{\mathrm{d}x} EG_B(x) = \sum_{n=0}^{\infty} B_{n+1} \frac{x^n}{n!}. \tag{2}$$

Substituera sedan in vår rekursion (1) i (2), och observera att det ni får ser väldigt mycket ut som exponentiella genererande funktionen för binomialfaltningen mellan Bell-talen och någon annan följd.

Använd detta för att få fram en differentialekvation för EG_B – lös den för att få fram ett uttryck för exponentiella genererande funktionen för Bell-talen.[22,23]

[22] Som vanligt behöver ni inte faktiskt ange hur ni löser den – bara skriv vad lösningen är.

[23] Ni har härmed lyckats plocka fram en EGF för en följd där vi faktiskt inte har något enkelt uttryck för vad varje enskild term blir – det finns inget fint uttryck för B_n i termer av n. Hade vi kunnat mer komplexanalys hade vi kunnat använda detta för att få fram skattningar för hur snabbt Belltalen växer, till exempel. (Svaret är: "väldigt väldigt snabbt", men vi hade kunnat vara precisare än så.)

Föreläsning 7: Dyck-stigar och Catalantal · 1MA020

Vilhelm Agdur[1]

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

14 februari 2023

Vi introducerar Dyck-stigar, och härleder en rekursion för deras antal. Sedan använder vi rekursionen för att hitta en genererande funktion, och använder genererande funktionen för att ge en explicit formel för deras antal.

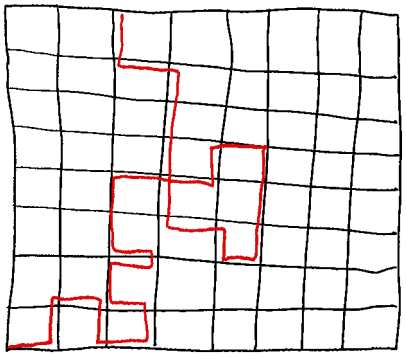
Efter det ger vi ett kombinatoriskt bevis för vår formel för antalet Dyck-stigar, som är betydligt kortare.

Slutligen ger vi två till exempel på saker som räknas av Catalantalen.

Dyck-stigar

Definition 1. En *gitterstig* på $\mathbb{Z}^2$ av längd n mellan a och b börjar i punkten a och tar sig sedan till punkten b med n stycken steg, som kan vara upp, ner, höger, eller vänster.[2]

[2] Vi kan betrakta en sådan stig som ett ord av längd n ur alfabetet $\{U, N, H, V\}$, tillsammans med en startpunkt.



Figur 1: En gitterstig av längd 28 från $(0,0)$ till $(2,8)$.

Det finns uppenbarligen 4^n gitterstigar av längd n med en given startpunkt, om vi inte kräver att den skall sluta i någon given punkt.

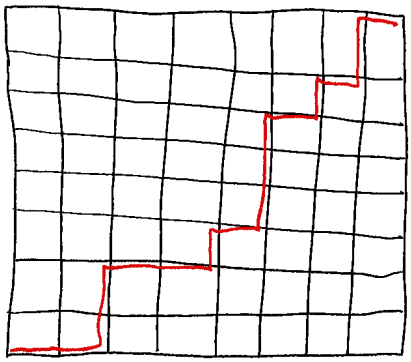
Definition 2. En *uppåt-höger-stig* på $\mathbb{Z}^2$ från a till b är en gitterstig mellan a och b som enbart tar steg uppåt och åt höger.[3]

[3] I tolkningen av stigar som ord är alltså dessa ord ur det mindre alfabetet $\{U, H\}$.

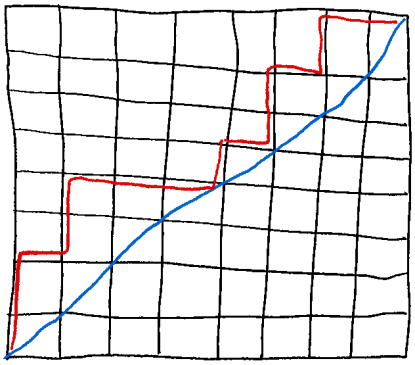
Notera att till skillnad från allmänna gitterstigar bestäms en uppåt-höger-stigs längd av dess start och slutpunkt, eftersom den inte kan ta några omvägar eller gå baklänges. En stig från $(0,0)$ till (a,b) kommer alltid att ta precis a steg uppåt och b steg till höger, det enda som kan variera är i vilken ording stegen tas.

Alltså ges det totala antalet uppåt-höger-stigar från $(0,0)$ till (a,b) av $\binom{a+b}{a}$, eftersom det är antalet sätt att välja de a ställen vi tar ett steg höger av totalt $a+b$ steg.

Definition 3. En Dyck-stig av längd $2n$ är en uppåt-höger-stig från $(0,0)$ till (n,n) som aldrig går under diagonalen.



Figur 2: En uppåt-höger-stig från $(0,0)$ till $(8,8)$ av längd sexton.



Figur 3: En Dyck-stig av längd sexton.

Notera att en Dyck-stig alltid måste börja med ett steg uppåt och sluta med ett steg åt höger, eftersom den annars ju hade varit under diagonalen.

Hur många Dyck-stigar finns det av varje given längd? Vi kan använda vår observation om att de alltid börjar med ett upp-steg för att ge en rekursion för detta antal:

Lemma 4. *Låt d_n beteckna antalet Dyck-stigar av längd $2n$. Då gäller det för alla $n \geq 0$ att*

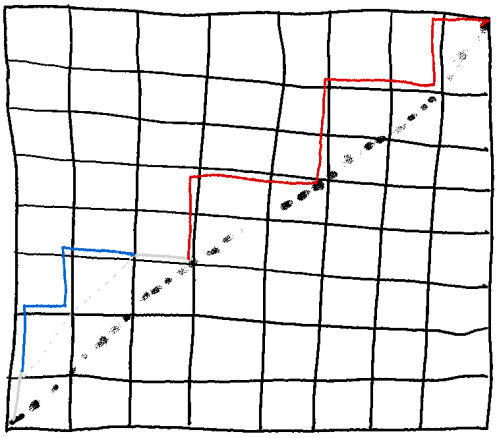
$$d_{n+1} = \sum_{k=0}^{n} d_k d_{n-k}$$

och $d_0 = 1$.[4]

[4] Antalet ord av längd noll anser vi vara ett, eftersom det bara finns ett sätt att välja ett sådant.

Bevis. Överväg en Dyck-stig av längd $2(n+1)$. Vi kan dela upp den i två kortare Dyck-stigar som följer: Den börjar med ett upp-steg, som vi färgar grått. Sedan fortsätter den i ett tag tills den träffar diagonalen för första gången. Vi färgar alla steg innan det steg i vilken den träffar diagonalen röda, och steget i vilken den träffar diagonalen grått. Sedan färgar vi resten av stegen blåa.

Vi hävdar att de blå stegen utgör en Dyck-stig av längd $2k$ för något $0 \leq k \leq n$, och de röda stegen utgör en Dyck-stig av längd $2(n-k)$, så att vi tillsammans med de två gråa stegen har totalt



Figur 4: En illustration av vår uppdelning av en Dyck-stig i gråa, blåa, och röda steg.

$2k + 2(n-k) + 2 = 2(n+1)$ steg. Ekvivalent, i tolkningen av stigar som ord, så säger vi att ordet för stigen vi började med kan skrivas som

$$Uw_1Hw_2$$

för två kortare[5] Dyck-stigar w_1 och w_2.

[5] Det är tillåtet att de är av längd noll.

Vi kan välja k fritt mellan 0 och n, och vi kan sedan välja våra två kortare Dyck-stigar helt fritt så länge de har rätt längd, så multiplikations- och additionsprincipen ger oss att vi kan totalt välja på

$$\sum_{k=0}^{n} d_k d_{n-k}$$

sätt, vilket är vad vi ville bevisa. □

Den uppmärksamme bland er kanske redan känt igen att den här rekursionen säger något om en faltning – specifikt säger den att

$$d_{n+1} = (d * d)_n,$$

vilket ser ut som något vi borde kunna använda för att räkna ut genererande funktionen av den här följden.

Proposition 5. *Den genererande funktionen för $\{d_k\}_{k=0}^{\infty}$, antalet Dyck-stigar, är*

$$F_d(x) = \frac{1 - \sqrt{1-4x}}{2x}.$$

Bevis. Vi observerar att Lemma 4 ger oss att för alla $n \geq 0$

$$d_{n+1} = (d * d)_n,$$

så om vi tar genererande funktioner av bägge sidorna ser vi att vänster led blir

$$\sum_{n=0}^{\infty} d_{n+1}x^n = \frac{1}{x}\sum_{n=1}^{\infty} d_n x^n = \frac{F_d(x) - 1}{x}$$

och höger led blir

$$F_{d*d}(x) = F_d(x)^2$$

så att vi har att

$$F_d(x) = xF_d(x)^2 + 1.$$

Det här är ju bara en vanlig andragradsekvation som vi kan lösa för F_d, och få att

$$F_d(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Det enda som återstår är att se om den rätta lösningen har ett plus- eller minustecken. Sättet vi ser detta på är att vi vet vad den skall ta för värde i en specifik punkt – vi kan ju nämligen räkna att

$$F_d(0) = \sum_{k=0}^{\infty} d_k 0^k = d_0 = 1$$

så funktionen måste vara ett i noll.

En snabb räkning ger oss att

$$\lim_{x\to 0} \frac{1-\sqrt{1-4x}}{2x} = 1$$

emedan gränsvärdet

$$\lim_{x\to 0} \frac{1+\sqrt{1-4x}}{2x}$$

inte existerar. Alltså måste den korrekta lösningen vara med minustecknet, såsom önskat. □

Så, hittills har vi definierat våra Dyck-stigar, listat ut en rekursion för deras antal, och använt denna rekursion för att härleda en genererande funktion. Kan vi använda denna genererande funktion för att härleda en explicit formel för antalet Dyck-stigar?

Svaret på den frågan är ja, men det kräver ett lemma vi inte sett ännu.

Newtons binomialsats, och en explicit formel för d_n

Definition 6. För varje $x \in \mathbb{R}$ och varje $k \in \mathbb{Z}^{\geq 0}$ ges den *fallande fakulteten* $x^{\underline{k}}$ av[6]

$$x^{\underline{k}} = x(x-1)(x-2)\dots(x-k-1)$$

och den *stigande fakulteten* $x^{\overline{k}}$ av

$$x^{\overline{k}} = x(x+1)(x+2)\dots(x+k-1).$$

Om x är ett heltal ges alltså $x^{\underline{k}}$ av $\frac{x!}{k!}$ och $x^{\overline{k}}$ av $\frac{(x+k-1)!}{(x-1)!}$.

[6] Så produkten har k termer. I fallet med $k = 0$ får vi en tom produkt, vilket vi konventionellt anser är ett, så $x^{\underline{0}} = x^{\overline{0}} = 1$ för alla x.

Vi kan särskilt notera att när x är ett heltal ges antalet permutationer av längd k ur ett alfabete med x bokstäver alltså av $x^{\underline{k}}$, och således har vi också att

$$\binom{x}{k} = \frac{x^{\underline{k}}}{k!}$$

för alla heltal x och k. Men detta uttrycket är ju helt väldefinierat även om x inte är ett heltal, vilket motiverar oss att göra följande definition:

Definition 7. För alla $x \in \mathbb{R}$ och $k \in \mathbb{Z}^{\geq 0}$ säger vi att

$$\binom{x}{k} = \frac{x^{\underline{k}}}{k!}.$$

Anledningen att vi gör allt detta arbetet är att det låter oss generalisera binomialsatsen även till potenser som inte är heltal, såsom Newton upptäckte.

Teorem 8 (Newtons binomialsats)**.** *För alla x och y och $r \in \mathbb{R}$ gäller det att*

$$(x+y)^r = \sum_{k=0}^{\infty} \binom{x}{k} x^{r-k} y^k$$

Bevis. Taylorutveckla.[7] □

[7] Ett bevis återfinns lätt med google, men eftersom det inte egentligen har något med kombinatorik att göra utelämnar vi det i denna kursen.

Låt oss nu tillämpa vår nya kunskap på Dyckstigarna. Eftersom den genererande funktionen vi fann för deras antal involverade en kvadratrot kommer vi ju vilja tillämpa Newtons binomialsats i fallet med $r = \frac{1}{2}$, så låt oss börja med ett lemma om vad som händer i just det fallet.

Proposition 9. *Antalet Dyck-stigar av längd $2n$, d_n, ges av*

$$d_n = 2(-1)^{n+1} \binom{1/2}{n+1} 4^n.$$

Bevis. Vi vet att den genererande funktionen för denna följd ges av

$$F_d(x) = \sum_{k=0}^{\infty} d_k x^k = \frac{1 - \sqrt{1-4x}}{2x}$$

så vi behöver serieutveckla detta uttryck.

Newtons binomialsats säger oss att

$$\sqrt{1+y} = \sum_{k=0}^{\infty} \binom{1/2}{k} y^k$$

så om vi sätter in $y = -4x$ får vi att

$$\sqrt{1-4x} = \sum_{k=0}^{\infty} (-1)^k \binom{1/2}{k} 4^k x^k.$$

När $k = 0$ så blir $\binom{1/2}{0} = \frac{(1/2)^{\underline{0}}}{0!} = \frac{1}{1}$, och alltså är hela nollte termen lika med ett. Så alltså gäller det att

$$\begin{aligned}\frac{1-\sqrt{1-4x}}{2x} &= \frac{\sum_{k=1}^{\infty}(-1)^k\binom{1/2}{k}4^k x^k}{2x} \\ &= \sum_{k=1}^{\infty} 2(-1)^k\binom{1/2}{k}4^{k-1}x^{k-1} \\ &= \sum_{k=0}^{\infty} 2(-1)^{k+1}\binom{1/2}{k+1}4^k x^k\end{aligned}$$

vilket genom att jämföra koefficienter ger oss resultatet. □

Så vi har hittat *en* formel, men den är inte särskilt vacker. Även om vi intellektuellt vet att den borde ge oss heltal är det inte alls uppenbart, med den fraktionella binomialkoefficienten och allt.

Kan vi hitta en vackrare formel? Svaret är ja, och det finns flera sätt för oss att göra det. Om vi hade haft mer uthållighet med krångliga räkningar hade vi kunna bevisa följande lemma, vilket låter oss förenkla uttrycket vi fick i Proposition 9:

Lemma 10. *Det gäller att*

$$\binom{1/2}{n} = \frac{(-1)^{n+1}}{4^n(2n-1)}\binom{2n}{n}.$$

Bevis. Utelämnas. Om du verkligen vill se en räkning för detta finns det ett bevis för något snarlikt, som borde gå att förenkla till detta, på stackexchange.[8] □

[8] Brian M. Scott (https://math.stackexchange.com/users/12042/brian-m scott). Binomial coefficients $\binom{1/2}{k}$. Mathematics Stack Exchange, 2020. URL `https://math.stackexchange.com/q/340141`. URL:https://math.stackexchange.com/q/340141 (version: 2020-03-27)

När vi tagit detta Lemma 10 och stoppat in det i Proposition 9 får vi följande mycket vackrare formel:

Teorem 11. *Antalet Dyck-stigar d_n ges av*

$$d_n = \frac{1}{n+1}\binom{2n}{n}.$$

I själva verket är dessa tal så viktiga att de har sitt egna namn – de kallas för Catalan-talen.

Så vi har till slut hittat en fin formel för antalet Dyck-stigar, och alltså för Catalantalen. Tyvärr var vägen vi tog dit väldigt lerig, i botten på en hopväxt och snårig dal. Finns det ett mindre kladdigt sätt att hitta denna formel?[9]

[9] Vårt arbete med att ta fram denna formel för antalet Dyck-stigar illustrerar både för- och nackdelarna med metoden med genererande funktioner. Det är en pålitlig metod, med tydliga steg för vad vi vill göra – efter att vi hittade rekursionen vi började med behövde vi aldrig egentligen vara kreativa, utan vi kom fram till målet genom att bara följa vårt recept.

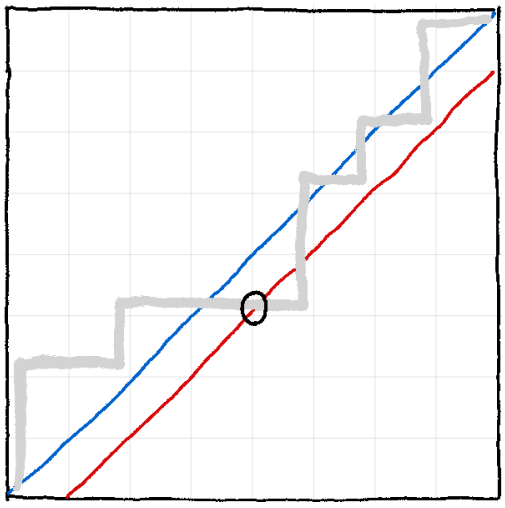
Å andra sidan kan räkningarna man behöver göra för att tillämpa metoden vara väldigt fula. Vad man köper i standardisering får man betala för i begriplighet – det är nog svårt att säga att man begriper *varför* den formeln ger Catalantalen efter att ha sett vårt bevis.

Ett kombinatoriskt bevis för formeln för Catalantalen

Ett kombinatoriskt bevis av Teorem 11. Låt oss överväga samlingen av alla uppåt-höger-stigar från $(0,0)$ till (n,n). Vi kallar varje stig som

passerar under diagonalen för en *dålig* stig – mängden av sådana är uppenbarligen komplementet till mängden av Dyck-stigar. Så om vi kan räkna de dåliga stigarna får vi också antalet Dyck-stigar, eftersom vi vet att det totala antalet uppåt-höger-stigar från $(0,0)$ till (n,n) är precis $\binom{2n}{n}$.

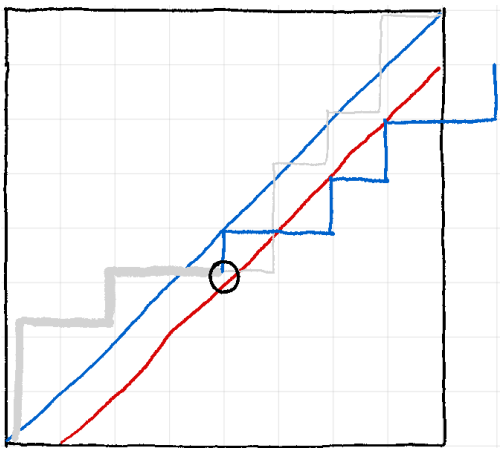
Sättet vi räknar antalet dåliga stigar är att påvisa en bijektion mellan dem och mängden av uppåt-höger-stigar från $(0,0)$ till $(n+1, n-1)$.



Figur 5: En av våra dåliga stigar, huvuddiagonalen med iblått och första diagonalen under huvuddiagonalen i rött. Punkten där stigen träffar den första underdiagonalen markeras med en cirkel.

Givet en dålig stig markerar vi första punkten på vilken den träffar första underdiagonalen, alltså diagonalen under huvuddiagonalen. Att det måste finnas en sådan punkt följer av att stigen är dålig – om den aldrig träffade den underdiagonalen vore stigen en Dyckstig.

Sedan speglar vi resten av stigen, efter punkten vi markerade, i första underdiagonalen. Vi ersätter alltså varje steg uppåt med ett steg till höger, och varje steg till höger med ett steg uppåt.



Figur 6: Den uppåt-höger-stig från $(0,0)$ till $(n+1, n-1)$ som motsvarar vår dåliga stig i förra figuren. Stigen är grå fram tills punkten där vi började spegla den, och fortsätter sedan i blått. Originalstigen fortsätter i grått.

Eftersom vi i punkten vi började spegla just träffat första underdiagonalen så måste vi i den punkten ha haft ett steg mer åt höger än uppåt. Totalt har vi, i originalstigen, lika många steg uppåt som åt höger, så återstoden av den efter den punkten måste ha ett steg mer uppåt än åt höger.

När vi speglar blir varje steg uppåt ett åt höger, och vice versa, så vår speglade stig måste ha ett steg mer åt höger än uppåt också i biten efter speglingen. Alltså måste den resulterande stigen efter speglingen ha två steg fler åt höger än uppåt, och alltså hamna i $(n+1, n-1)$.[10]

Så vi har hittat ett sätt att skicka en dålig stig på en stig från $(0,0)$ till $(n+1, n-1)$. För att detta skall vara en bijektion måste processen vara reversibel - givet en stig från $(0,0)$ till $(n+1, n-1)$ måste vi kunna återskapa den motsvarande dåliga stigen.

Sättet vi gör det på är samma som innan – vi hittar första punkten i vilken vår stig träffar första underdiagonalen, och speglar efter den. Att en sådan punkt måste finnas är uppenbart, eftersom $(0,0)$ ligger ovanför den underdiagonalen, och $(n+1, n-1)$ ligger under den. Så för att ta oss från ena sidan av den till andra måste vi passera den.

Att denna spegling kommer ge oss rätt dåliga stig är enkelt att se – allt vi gjort är att spegla två gånger, vilket så klart inte gör någonting.

Alltså har vi bevisat att antalet dåliga stigar är lika med antalet stigar från $(0,0)$ till $(n+1, n-1)$. Vi vet att det finns $\binom{(n+1)+(n-1)}{n+1}$ sådana stigar, så vi kan räkna att

$$\begin{aligned} d_n &= |\text{stigar } (0,0) \to (n,n)| - |\text{dåliga stigar}| \\ &= \binom{2n}{n} - \binom{2n}{n+1} \\ &= \frac{(2n)!}{n!n!} - \frac{(2n)!}{(n+1)!(n-1)!} \\ &= (2n)!\left(\frac{(n+1)}{(n+1)!n!} - \frac{n}{(n+1)!n!}\right) \\ &= \frac{(2n)!}{(n+1)!n!} = \frac{1}{n+1}\frac{(2n)!}{n!n!} = \frac{1}{n+1}\binom{2n}{n} \end{aligned}$$

vilket bevisar satsen. □

Så vårt kombinatoriska bevis undvek helt att behöva fundera på rekursioner och genererande funktioner. Det är en mycket mer direkt rutt till vårt mål, men vi missade några sevärdheter längs vägen.[11]

Fler saker som räknas av Catalantalen

Som vi nämnde tidigare är Catalantalen viktiga eftersom de räknar fler saker än bara just Dyck-stigar. I nästa föreläsning kommer vi

[10] I symboler har vi u_i steg *u*ppåt i stigen *i*nnan punkten vi speglar efter, och h_i steg åt *h*öger. Efter punkten vi speglar *e*fter har vi u_e steg uppåt och h_e steg åt höger. Så i Figur 5 så har vi $u_i = 3$, $h_i = 4$, $u_e = 5$, och $h_e = 4$.

Så för stigen vi börjar med har vi $h_i = u_i + 1$, och $h_i + h_e = n$ samt $u_i + u_e = n$ för att den skall sluta i (n, n). Stigen efter speglingen kommer att ha $h_i + u_e$ steg åt höger och $u_i + h_e$ steg uppåt. Om man arbetar sig igenom dessa ekvationer kommer man att se att vi verkligen har $n+1$ steg åt höger och $n-1$ steg uppåt i den reflekterade stigen.

[11] Hur man hade härlett vår rekursion eller den genererande funktionen givet bara vad vi lärde oss i det kombinatoriska beviset är långt ifrån uppenbart.

se ett viktigt exempel. Nu, i slutet på denna, tar vi några mindre exempel.

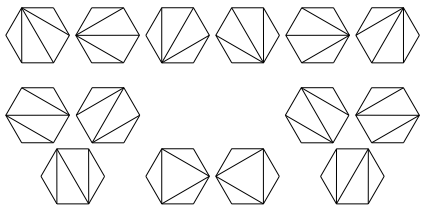
Exempel 12. Antalet sätt att skriva $2n$ matchande parenteser räknas av Catalantalen. Med matchande parenteser menar vi alltså ett uttryck som $(()(()))()(())$ – och i ett uttryck som $)((()$ matchar de inte. Varje $($ måste ha en motsvarande $)$ senare i ordet, och varje $)$ måste ha ett matchande $($ senare i ordet.

Hur bevisar vi att detta räknas av Catalantalen? Jo, vi ser att detta lyder samma rekursion som Dyck-stigarna gjorde. Varje uttryck med matchande parenteser måste börja med $($, och denna första startparentes måste matcha en slutparentes. Det som står inom dessa parenteser måste också vara ett matchande uttryck, och likaså det som står efter slutparentesen som matchar första parentesen.

Alltså kan vi skriva varje uttryck med matchande parenteser på formen $(w_1)w_2$, med w_1 och w_2 två kortare matchande uttryck. Det här är precis samma uppdelning som vi hade för våra Dyckstigar, så det kommer ge samma rekursion, och alltså är det samma följd.[12]

[12] Vi hade också, vilket kanske vore enklare, helt enkelt kunnat se att det finns en bijektion mellan matchande uttryck med parenteser och Dyck-stigar, genom att tolka $($ som "steg uppåt" och $)$ som "steg till höger".

Exempel 13. Det problem som ursprungligen fick upp matematikers intresse i väst[13] för Catalantalen var att dela upp en konvex polygon med $n+2$ sidor i trianglar, genom att rita streck mellan hörnen som inte korsar varandra.



Figur 7: Fallet med hexagoner.

[13] De studerades först av en matematiker i Kina på 1700-talet vid namn Minggatu, som använde dem för att ge identiteter för sinus-funktionen, i stil med

$$\sin(2\alpha) = 2\sin(\alpha) - \sum_{n=1}^{\infty} \frac{C_{n-1}}{4^{n-1}} \sin^{2n+1}(\alpha).$$

Det här problemet studerades först av Euler[14], och beviset att de räknas av Catalantalen utvecklades av Segner, Goldbach, och Lamé. Vår rekursion för Catalantalen brukar kallas för Segnerrekursionen.

Senare studerades problemet med parentetiseringar av Eugène Charles Catalan, efter vilken talen fick sitt namn på femtiotalet.

[14] Som ju redan har mer än tillräckligt med saker namngivna efter sig, så det är tur att vi inte döpte talen efter honom.

Övningar

Övning 1. Hur många gitterstigar av längd n från $(0,0)$ till (a,b) finns det?

Övning 2. Bevisa att antalet uppdelningar av en konvex polygon med $n+2$ sidor i trianglar, såsom vi diskuterade i Exempel 13, räknas av Catalantalen.[15]

[15] Ledtråd: Tänk kombinatoriskt, och se att dessa också lyder vår rekursion.

Övning 3. Betrakta mängden av följder av heltal av längd n, som

- börjar med 1,
- och om det föregående talet är k är nästa tal vilket tal som helst mellan 1 och $k+1$.

För $n = 4$ är dessa följder

1234, 1233, 1232, 1231, 1223, 1222, 1221, 1212, 1211, 1123, 1122, 1121, 1112, 1111.

Bevisa att antalet av dessa följder ges av Catalantalen.

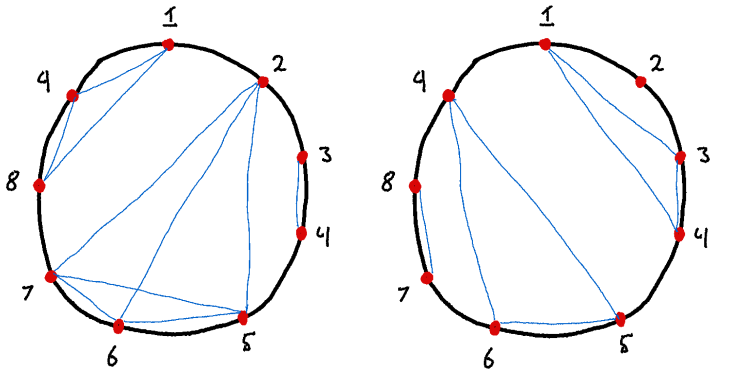
Övning 4. Bevisa att alla följderna på denna lista är lika med Catalantalen:

1. Antalet ord ur alfabetet $\{-1, 1\}$ med n stycken av varje bokstav, sådana att alla partialsummor är ickenegativa. Det vill säga, om vi tar summan av de första k bokstäverna i ordet skall det inte bli negativt, för alla $0 \leq k \leq 2n$.
2. Följder $1 \leq a_1 \leq a_2 \leq \ldots \leq a_n$ av heltal, med $a_i \leq i$ för alla i.
3. En valfri följd från Richard Stanleys lista av 66 saker som räknas av Catalantalen[16], som inte redan dykt upp i föreläsningen eller i en annan övning.

[16] Denna lista återfinns här: `https://math.mit.edu/~rstan/ec/catalan.pdf`

Övning 5. Vi skriver talen 1 till n i ordning runt en cirkel.[17] Vi säger att en mängdpartition $\{A_1, A_2, \ldots, A_k\}$ av $[n]$ är *ickekorsande* ifall det, när vi ritar streck mellan alla tal som ligger i samma del av partitionen, aldrig händer att två streck som hör till olika delar korsar varandra. Alltså, närhelst $a, b \in A_i$ och $c, d \in A_j$ så korsar inte strecket ab strecket cd. Se figur 8 för två exempel på ickekorsande partitioner då $n = 9$, och figur 9 för ett exempel på en korsande partition.

[17] Visst är ni glada att jag inte valde att formulera detta som "n personer runt ett runt bord?"?

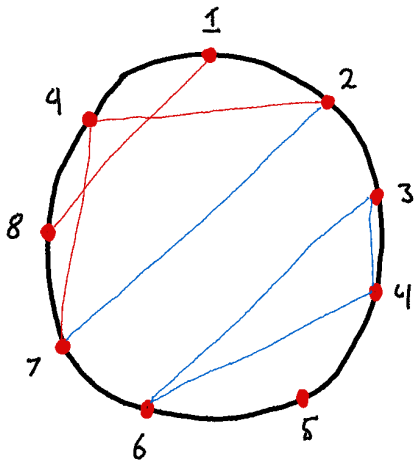


(a) $\{\{1,8,9\},\{2,5,6,7\},\{3,4\}\}$. (b) $\{\{1,3,4\},\{2\},\{5,6,9\},\{7,8\}\}$.

Figur 8: Två stycken ickekorsande mängdpartitioner.

Bevisa att antalet ickekorsande partitioner räknas av Catalantalen.[18]

[18] Ledtråd: Fundera på strecket mellan 9 och 5 i den högra av våra två exempel på ickekorsande partitioner. Kan ni se en rekursion?



Figur 9: Den korsande partitionen $\{\{1,8\},\{2,7,9\},\{3,4,6\},\{5\}\}$, med de korsande strecken i rött.

Referenser

Brian M. Scott (https://math.stackexchange.com/users/12042/brian-m scott). Binomial coefficients $\binom{1/2}{k}$. Mathematics Stack Exchange, 2020. URL `https://math.stackexchange.com/q/340141`. URL:https://math.stackexchange.com/q/340141 (version: 2020-03-27).

Föreläsning 8: Grafer och träd · 1MA020

Vilhelm Agdur[1]

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

16 februari 2023

Vi introducerar grafer och träd, och bevisar att antalet rotade ordnade binära oetiketterade träd också räknas av Catalantalen. Vi bevisar också att samlingen av alla oetiketterade ordnade träd räknas av Catalantalen, fast på ett lite annat sätt.

Efter det bevisar vi Cayleys formel, som säger att det finns n^{n-2} etiketterade träd på n noder, på två olika sätt.

Grafer och träd

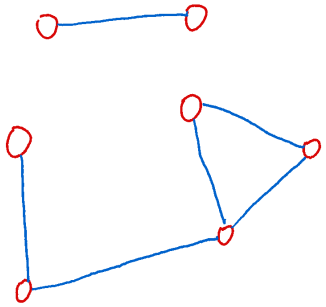
Vårt första ämne i denna föreläsning är grafer och träd, som kommer dyka upp igen och igen också i senare föreläsningar – det är ju till och med den preliminära titeln på vår sista föreläsning. Vi börjar med att ge en samling definitioner av vad vi menar med dessa ord, och sedan börjar vi räkna hur många av olika typer av graf det finns i olika klasser.

Definition 1. En *graf* består av en mängd V av *noder* och en mängd $E \subseteq \binom{V}{2}$ av kanter.[2] Om det finns en kant $\{u, v\}$ säger vi att u och v är *grannar*. En graf är *etiketterad* om noderna är särskiljbara, annars är den oetiketterad. [3] Vi säger att en graf är *sammanhängande* om det går att nå varje nod från varje annan nod genom att vandra längs kanterna. Ett sätt att vandra från en nod tillbaka till sig själv kallar vi för en *cykel*.

[2] Med notationen $\binom{A}{k}$ där A är en mängd och k ett heltal menar vi *mängden* av delmängder av storlek k till n. Alltså har vi att

$$\left|\binom{[n]}{k}\right| = \binom{n}{k}.$$

[3] Det här är precis samma koncept som med våra lådor som var särskiljbara eller inte. Antingen har noderna namn, så vi kan prata om nod nummer tre, eller så kan vi bara se vilka andra noder de har kanter till.



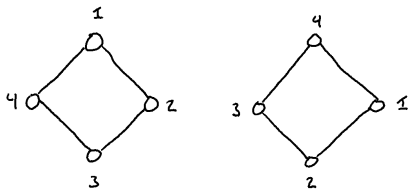
Figur 1: Ett exempel på en graf. Den är inte sammanhängande, eftersom de övre två noderna inte kan nås från de undre fem. Triangeln utgör en cykel, som är grafens enda.

Exempel 2. Det finns $2^{\binom{n}{2}}$ stycken etiketterade grafer på n noder, eftersom det finns $\binom{n}{2}$ möjliga kanter, och vi får en graf per val av vilka kanter som skall vara med.

Problemet med att räkna antalet oetiketterade grafer på n noder är betydligt mer komplicerat. Den första idén man hade haft är kanske att det borde vara

$$\frac{2^{\binom{n}{2}}}{n!}$$

eftersom det borde finnas $n!$ olika sätt att sätta dit etiketterna. Problemet är att vissa grafer har symmetrier som gör att till synes olika sätt att skriva dit etiketter i själva verket ger samma etiketterade graf.



Figur 2: Två till synes olika etiketteringar av samma graf, som i själva verket är samma etikettering på grund av grafens rotationssymmetri.

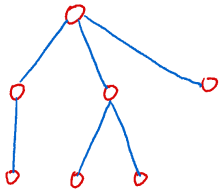
Som tur är visar det sig att nästan alla grafer inte har någon symmetri alls, så svaret är *nästan* $\frac{2^{\binom{n}{2}}}{n!}$.[4]

[4] Det här påståendet låter kanske löst i kanten, men det är faktiskt helt rigoröst. I alla fall om man ersätter "nästan" med att skriva att antalet är

$$(1+o(1))\frac{2^{\binom{n}{2}}}{n!}.$$

Definition 3. Ett *träd* är en sammanhängande graf utan cykler. Ett *rotat* träd är ett träd med en specifik nod utpekad som dess rot.[5] I ett rotat träd har varje nod utom roten själv en granne som är närmre roten än sig[6], vilken vi kallar dess *förälder*. Alla dess andra grannar kallar vi dess *barn*. En nod utan barn kallar vi för ett *löv*, och en nod som inte är ett löv kallar vi för *intern*.

Ifall det spelar roll i vilken ordning vi ritat noderna kallar vi trädet *ordnat*, se figur 4.

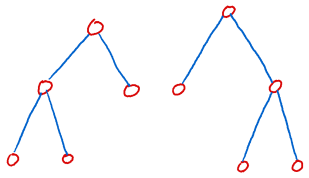


Figur 3: Ett träd med sju noder och sex kanter.

[5] Så om trädet är oetiketterat kan vi alltså se vilken nod som är roten, men resten av noderna kan vi inte se skillnad på, bara vilka som hänger ihop med vilka med kanter.

[6] Eller är roten.

Definition 4. Ett träd i vilket alla noder antingen har två eller noll barn kallas för ett *binärt* träd.



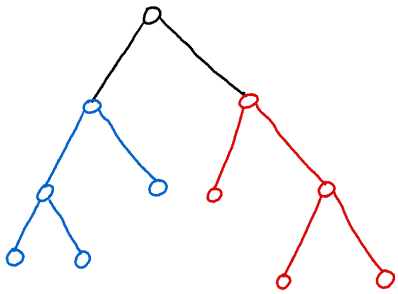
Figur 4: Två träd som är olika varandra som ordnade träd, men samma träd som oordnade träd.

Ännu fler saker som räknas av Catalantalen

Låt oss nu återse en gammal vän, Catalantalen.

Proposition 5. *Antalet rotade ordnade binära oetiketterade träd med n stycken interna noder ges av Catalantalen.*

Bevis. Vi kan dela upp ett sådant träd i två mindre träd genom att helt enkelt ta bort roten, och låta dess två barn vara rötter i två mindre träd.



Figur 5: Ett rotat ordnat binärt oetiketterat träd, med uppdelningen av det i två mindre träd av samma typ, ett rött och ett blått.

Alltså gäller det, om t_n betecknar antalet sådana träd, att

$$t_{n+1} = \sum_{k=0}^{n} t_k t_{n-k},$$

eftersom vi kan skapa oss ett sådant träd med $n+1$ noder genom att först rita roten, och sedan fästa ett träd med k interna noder till vänster och ett med $n-k$ interna noder till höger. Eftersom roten själv är intern har vi då $k+n-k+1 = n+1$ interna noder. □

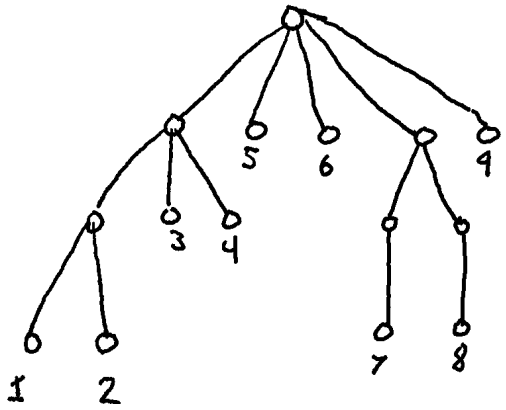
I själva verket räknas också godtyckliga oetiketterade ordnade träd av Catalantalen, utan något krav på att de skall vara binära.

Proposition 6. *Antalet rotade ordnade oetiketterade träd på $n+1$ noder ges av Catalantalen.*[7]

[7] Notera att vi här räknar *alla* noder, inte bara de interna, som vi gjorde för de binära träden.

Bevis. Vi bevisar detta genom att uppvisa en bijektion med sätt att skriva n matchande par av parenteser.

Så, givet ett rotat ordnat oetiketterat träd på $n+1$ noder, numrera dess löv från höger till vänster.



Figur 6: Ett rotat ordnat oetiketterat träd, med dess löv numrerade från vänster till höger.

I vår algoritm för att omvandla detta träd till en parentetisering blir uttrycket, innan vi ersatt talen med $()$,

$$((12)34)56((7)(8))9.$$

Skriv sedan upp talen $12\ldots k$ på rad, och skriv i parenteser på följande vis: För varje intern nod, förutom roten, skriv ett par parenteser runt alla de tal som motsvarar löv under noden. Ersätt sedan varje av talen med ett tomt par av parenteser, $()$. Detta ger en parentetisering med precis n par av parenteser.

För att återhämta ett träd från en parentetisering, börja med att rita en nod för varje $()$. Sedan, för varje grupp av noder som ligger i samma par av parenteser, rita en gemensam förälder för dem. Till slut, rita dit roten, och koppla den till varje par av parenteser som inte har någon parentes runt sig. □

Cayleys formel

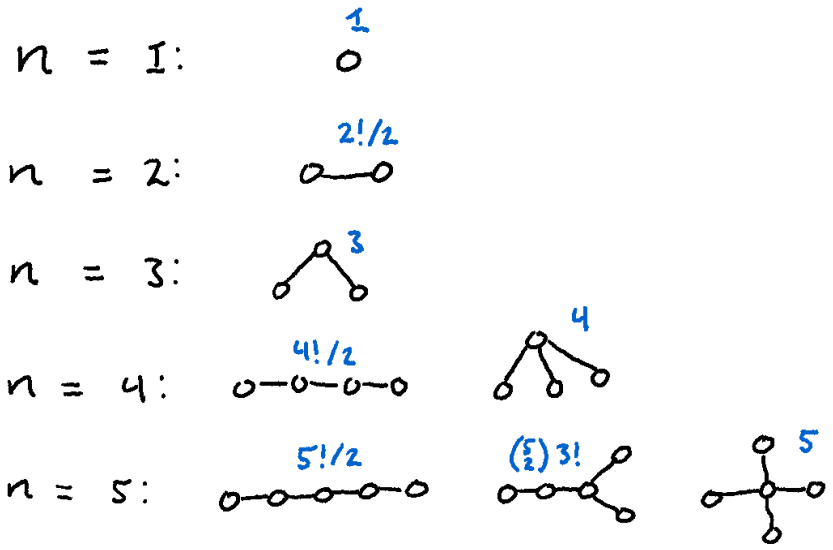
Vi har alltså lyckats räkna två specifika sorters träd. Kan vi räkna träd mer generellt?

Teorem 7. *Det finns*

$$n^{n-2}$$

stycken etiketterade träd med n noder.

För att förstå detta resultat, låt oss börja med att räkna de första små fallen. Vi kollar på *oetiketterade* träd, och räknar hur många sätt vi kan sätta etiketter på dem.



Figur 7: Oetiketterade grafer med n noder, för $n = 1, \ldots, 5$, med antalet sätt att sätta etiketter på varje i blått.

Sätten vi får dessa antal är, per värde på n:

1. Att det bara finns ett sätt att skriva en etta på den enda noden är uppenbart.
2. Vi kan välja vilken permutation som helst av $[2]$ att skriva på noderna, men grafen har en speglingssymmetri, så att skriva etiketterna i motsatt ordning ger samma träd. Alltså $\frac{2!}{2}$.
3. Vi kan se vilken nod som är den mellersta, men vi kan inte se skillnad på de två yttre. Alltså är det enda val vi kan göra det av vilket tal vi skriver på den mellersta, vilket vi kan välja på tre sätt.
4. För den första av våra två oetiketterade grafer kan vi skriva vilken permutation av $[4]$ vi vill, men återigen har vi en speglingssymmetri, så att skriva den baklänges ger oss samma etikettering. Alltså $\frac{4!}{2}$.

För den andra är vi i samma situation som vi var i för $n = 3$ – vi kan se vilken nod det är som har mer än en granne, men vi kan inte se skillnad på de andra. Alltså är det enda valet vi har vilken etikett just den särskilda noden får, vilket vi kan göra på 4 sätt.

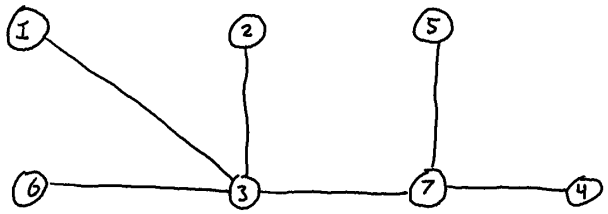
5. Vi får $\frac{5!}{2}$ av samma speglingssymmetri-skäl som innan, och för den tredje av våra grafer får vi 5 eftersom vi åter har en särskild nod och resten kan vi inte se skillnad på.

   För den mellersta av våra tre oetiketterade träd kan vi se skillnad på de tre noderna i svansen till vänster, men de två som sticker ut åt höger kan vi inte se skillnad på. Så för att etikettera denna väljer vi två etiketter för de talen, vilket vi kan göra på $\binom{5}{2}$ sätt, och sedan är varje permutation av de återstående tre etiketterna faktiskt en distinkt etikettering, så vi kan välja 3! sätt att fullfölja vår etikettering. Så vi har totalt $\binom{5}{2}3!$ sätt att göra detta på.

Så vi ser i alla fall att vår formel gäller för n upp till fem. Vi väljer att ge två bevis för denna sats. Det första är av Prüfer, och ger en bijektion mellan etiketterade träd och en enklare mängd.

Prüfers bevis av Cayleys formel (1918). Vi vill visa på en bijektion mellan mängden av etiketterade träd på n noder och mängden av ord av längd $n-2$ ur alfabetet $[n]$. Att den senare mängden har rätt antal element vet vi sedan innan, så om vi kan hitta en bijektion är vi klara.

Vi börjar med att berätta hur vi skapar vårt ord givet ett etiketterat träd.[8] Vi letar upp det löv[9] som har lägst etikett, skriver dess etikett som första bokstav i vårt ord, och tar sedan bort noden ur trädet.



Figur 8: Ett etiketterat träd med Prüferkod 33773.

Vi upprepar denna process – letar upp det löv i det resulterande trädet som har lägst etikett (och notera att vi, när vi tar bort ett löv, ibland kommer göra en nod som innan var intern till ett löv), skriver den etiketten på slutet av ordet, och tar bort lövet. Processen fortsätter tills vi bara har två noder kvar.

För att gå från en Prüferkod till en etiketterad graf använder vi följande algoritm, som konstruerar ett etiketterat träd givet en Prüferkod $a_1 a_2 \dots a_{n-2}$.

Det tar en stund att förstå vad den här algoritmen faktiskt gör[10], men efter en stunds kontemplation ser man att vad den gör är att

[8] Detta ord kallas för trädets *Prüferkod*.

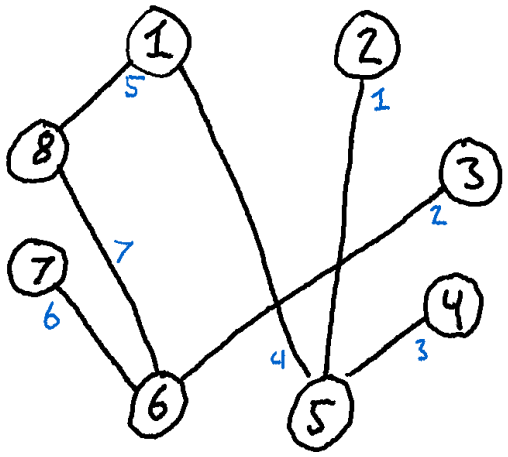
[9] Strikt sett har vi hittills bara definierat *löv* för rotade träd – och de träd vi studerar här har ju ingen rot-nod. Med "löv" menar vi här "nod med bara en granne".

[10] En fördel med föreläsningar över text är att man faktiskt kan genomföra algoritmen på ett konkret exempel, för att illustrera den, men en text måste så klart vara statisk. Sitter du hemma och läser föreslår jag att du prövar att göra algoritmen för hand på någon eller några Prüferkoder, för att få en känsla för vad som pågår.

Algorithm 1: Konstruktion av träd från Prüferkoder

Låt G vara en graf med n noder, med etiketter $1, 2, \ldots, n$, men utan kanter
$L_1 \leftarrow (1, 2, \ldots, n)$
$A_1 \leftarrow (a_1, a_2, \ldots, a_{n-2})$
for $t = 1, 2, \ldots$ **do**
  if $|L_t| = 2$ **then**
    Rita en kant i G mellan de två elementen i L
    stop
  else
    Låt l vara det minsta elementet i L_t som inte är i A_t
    Låt a vara det första elementet i A_t
    Rita en kant i G mellan l och a
    $L_{t+1} \leftarrow L_t \setminus \{l\}$
    $A_{t+1} \leftarrow (A_t(2), A_t(3), \ldots, A_t(|A_t|))$
  end if
end for
return G

den lägger till kanterna i precis den ordning som de försvann när vi skapade Prüferkoden.



Figur 9: Ett träd skapat från Prüferkoden 565186. I blått har vi markerat i vilket steg i algoritmen varje kant lades till – lägg märke till att detta är precis ordningen i vilken de *tas bort* om vi skapar Prüferkoden för detta trädet.

Den första kanten att ritas kommer gå mellan det första lövet att tas bort och dess granne, den andra går mellan andra lövet att tas bort och dess granne, och så vidare – ända fram tills den sista kanten vi lägger till, som går mellan de två kvarvarande noderna när vi byggde Prüferkoden. Alltså kommer denna algoritmen precis att rekonstruera grafen vi började med, vilket bevisar att vi faktiskt har en bijektion, och satsen följer. □

Ett alternativt bevis av Cayleys formel

Det bevis vi just gav av Cayleys formel är visserligen elegant, men det är inte det enda beviset av denna sats. Det finns åtskilliga andra bevis – inte bara med hjälp av bijektioner, utan också med rekursioner, och ett klassiskt bevis som använder determinanter och Kirchhoffs matris-träd-sats.

Beviset vi skall ge nu använder inga avancerade metoder alls, inte ens en bijektion, utan är bara ett helt vanligt "räkna på två sätt"-bevis. I boken jag tog det från [11] beskrivs detta som "det vackraste beviset av dem alla", men personligen föredrar jag nog Prüfers bevis, som inte ens var med på deras lista.

För att kunna ge detta bevis behöver vi definiera några till koncept.

Definition 8. En *riktad* graf är en graf där varje kant har en utpekad start- och slutnod. Vi tänker oss kanterna som pilar som pekar från start till slut.

Det finns ett uppenbart sätt att omvandla ett rotat träd till ett *riktat* träd[12] genom att ge varje kant den riktning som pekar bort från roten, och vice versa kan vi, för ett riktat träd med konsistenta riktningar på kanterna göra om det till ett rotat oriktat träd.

Definition 9. En graf H med noder V_H och kanter E_H är en *delgraf* till en graf $G = (V_G, E_G)$ om $V_H \subseteq V_G$ och

$$E_H \subseteq \{\{u, v\} \in E_G : u, v \in V_H\}.$$

För att skapa oss en delgraf till G tar vi alltså någon delmängd till dess noder, och tar sedan någon delmängd av kanterna mellan dessa noder.

Om graferna är riktade kräver vi att de skall ha samma riktning i G som i H. Om de är etiketterade kräver vi att etiketterna skall matcha i H och G.

Definition 10. En *skog* är en graf sådan att varje sammanhängande komponent är ett träd. Eller ekvivalent kan vi säga att det är en graf utan cykler.

En *rotad* skog är en skog med ett val av rot för varje träd i skogen.

Alternativt bevis av Cayleys sats. Låt $\mathcal{F}_{n,k}$ beteckna mängden av rotade skogar med n noder, som består av k träd. Alltså är $\mathcal{F}_{n,1}$ antalet rotade träd – om vi kan räkna dem är vi klara, eftersom vi vet att det finns precis n val av rot, så $\frac{|T_{n,1}|}{n}$ är talet vi söker.

Vi säger att en skog F' *ligger i* en annan skog F om F' är en delgraf till F när vi betraktar dem som riktade träd.[13]

Nyckelidén i vårt bevis är *klyvande följder* av rotade skogar. Vi säger att en följd $F_1, F_2, \ldots, F_k$ av rotade skogar på n noder är *klyvande* om varje F_i består av i stycken träd, och F_i innehåller F_{i+1} för varje i.

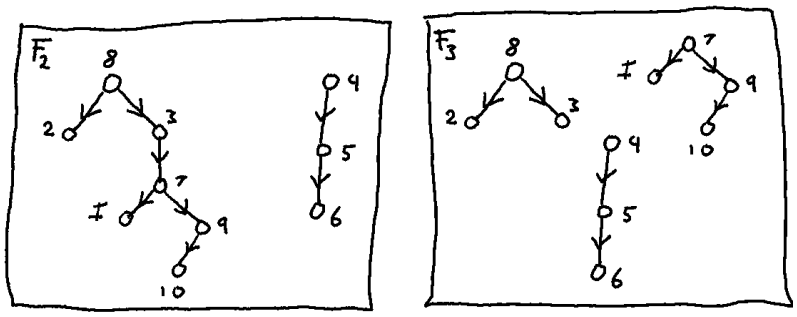
[11] Beviset är av Jim Pitman, men boken är *Proofs from the Book*. Den får detta namn från hur Erdős brukade påstå att Gud hade en bok som innehöll alla de vackraste bevisen. (Kanske en väldigt infantil version av de medeltida teologernas idéer om matematiken som Guds ordning i Hans skapelseverk?)

Hela idén om "boken" är egentligen lite märklig, med tanke på att Erdős var ateist – om än av typen som är arg på Gud för Hans påstådda ickeexistens.

Själva boken (den jag tog beviset ur, alltså) är, för övrigt, inte så särskilt bra, i min mening. Den gör bevisen mer komplicerade än de behöver vara, och har ett lite udda urval. Herren har definitivt en bättre bok, även om allvetande kanske får anses som fusk när man letar efter bevis.

[12] Alltså ett träd som har riktade kanter.

[13] Vi har ju inte definierat vad vi menar med att ett *rotat* träd skulle vara en delgraf till ett annat. För att vara tydliga betyder detta att vi *inte* kräver att roten till ett träd i F' också är rot till det större träd det ligger i i F.



Figur 10: Två rotade skogar F_2 och F_3, betraktade som riktade träd. Notera att F_3 ligger i F_2.

Låt nu $F_k \in \mathcal{F}_{n,k}$ vara en fix skog, och beteckna

- antalet rotade *träd* som innehåller F_k med $N(F_k)$, och
- antalet klyvande följder som slutar med F_k med $N^*(F_k)$.

Notera nu att om vi tar $k = n$ finns det bara ett val för F_k, nämligen skogen av n stycken träd, där varje träd bara är en enda nod – och *varje* rotat träd på n noder innehåller denna skog. Alltså är $N(F_n)$ helt enkelt antalet rotade träd, vilket ju är vad vi vill räkna.

Så om vi kan hitta en formel för $N(F_k)$ är vi klara. Vi gör detta genom att räkna $N^*(F_k)$ på två olika sätt. Först går vi från F_k till F_1, och sedan i motsatt riktning.

Givet ett F_k, hur många val har vi av av F_{k-1}? Eftersom F_{k-1} ska ha ett träd färre, måste vi foga ihop två träd med en kant. Den här kanten kan utgå från vilken nod som helst, och skall träffa en av de $k-1$ rötterna till andra träd än det träd noden själv är i.[14] I figur 10 kan vi till exempel få F_2 från F_3 genom att rita dit en kant från 3 till 7, som är roten för sitt träd.

[14] Den måste träffa en rot för att riktningen på kanterna skall förbli konsekvent – om den träffade en ickerot hade vi fått en nod som är slutnod för två kanter, och alltså har två föräldrar, vilket vi inte tillåter.

Vi kan alltså välja F_{k-1} givet F_k på $n(k-1)$ sätt. Precis samma argument ger att vi kan välja F_{k-2} givet F_{k-1} på $n(k-2)$ sätt, och så vidare. Så totalt kan vi välja vår följd $F_k, F_{k-1}, \ldots, F_1$ på

$$N^*(F_k) = n^{k-1}(k-1)!$$

sätt.

Så till den andra riktningen – givet F_k finns det, per definition, precis $N(F_k)$ val av F_1, eftersom F_1 skall vara något rotat träd som innehåller F_k. Vi ser enkelt att det är precis $k-1$ kanter som ligger i F_1 men inte i F_k – när vi räknade i motsatta riktningen är det dessa vi lade till.

Tar vi bort en av dessa kanter klyver vi F_1 och får en skog F_2, tar vi bort en till klyver vi ytterligare ett träd och får F_3, och så vidare – och varje klyvande följd $F_1, F_2, \ldots, F_k$ med fixt F_1 och F_k kan fås på detta vis.

Uppenbarligen är antalet sätt att välja en ordning att ta bort de

$k-1$ kanterna i precis $(k-1)!$, så vad vi har visat är att

$$N^*(F_k) = N(F_k)(k-1)!$$

vilket tillsammans med vårt andra sätt att räkna $N^*(F_k)$ ger oss att

$$N(F_k) = n^{k-1}.$$

Vi observerade innan att $N(F_n)$ är lika med det totala antalet rotade träd, och eftersom det finns n sätt att välja roten till ett träd är talet vi letar efter alltså

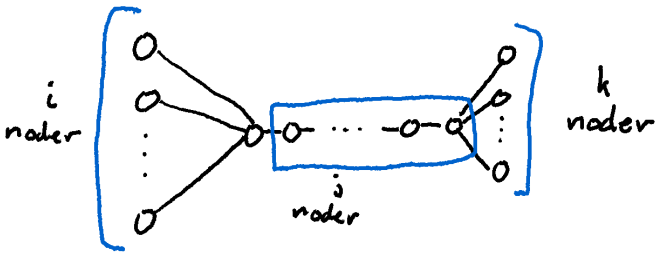
$$\frac{N(F_n)}{n} = \frac{n^{n-1}}{n} = n^{n-2}$$

såsom önskat. □

Övningar

Övning 1. Bevisa att ett träd alltid har $|E| = |V| - 1$.

Övning 2. Överväg följande skiss av ett oetiketterat träd med $1 + i + j + k$ noder:



Figur 11: Skiss av ett oetiketterat träd.

Hur många olika sätt finns det att sätta etiketter på detta träd?[15] Ge en formel som gäller för alla $i, j, k = 0, 1, 2, \ldots$.[16]

Övning 3. Rita det etiketterade trädet som har Prüferkod 1273262.

Övning 4. *En övning för dig som kan programmera.*[17] Implementera vår algoritm för att omvandla en Prüferkod till ett etiketterat träd i faktisk kod. Koden skall ge ett lämpligt grafobjekt som output, och en bild av grafen.[18]

Pröva din kod på några slumpmässigt valda Prüferkoder. Hur ser ett träd vanligtvis ut?

Övning 5. Betrakta figur 12, med fem olika riktade etiketterade grafer ritade. Vilka grafer är delgrafer till vilka?

Föreställ er nu att vi glömmer bort riktningen på alla kanterna, så att graferna blir *oriktade* etiketterade grafer. Hur förändras era svar?

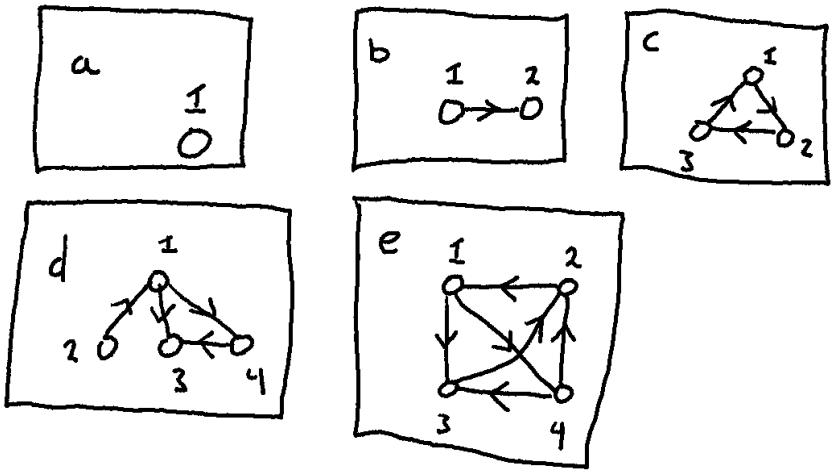
Om vår glömska fortsätter, och vi glömmer också etiketterna, hur ändras era svar? I det här fallet kan vi till och med ha att en graf är

[15] Vi resonerade om detta för några små träd precis efter att vi introducerade Cayleys formel, men här har vi alltså ett mer generellt fall.

[16] Finns det några specialfall för särskilda kombinationer av värden på i, j, och k?

[17] För inlämningsuppgiften i kursen är denna uppgift frivillig om ni inte har någon i er grupp som kan programmering. Om ni genomför den, vänligen använd inte Matlab, eftersom jag inte kan köra sådan kod. Mathematica är okej.

[18] Skriver du i R, C/C++, eller Python kan jag föreslå *igraph*-paketet för graf-datatypen och att rita dem. Mathematica har inbyggd funktionalitet för detta, så klart.



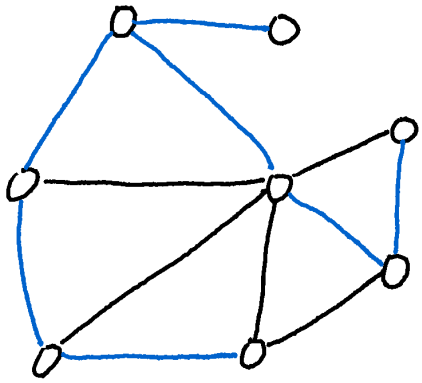
Figur 12: Fem olika riktade etiketterade grafer, a till e.

en delgraf till en annan på flera olika sätt – till exempel finns det nu två olika delgrafer till b som bägge är a (ta en av bs två noder), och c har tre delgrafer som är b (ta två av noderna och kanten mellan dem). Ange för varje par av grafer hur många olika sätt den ena är en delgraf till den andra, som oetiketterade grafer.

Övning 6. För varje n betecknar vi med K_n den *fullständiga grafen* på n noder, vilken är grafen med n noder med etiketter från 1 till n och varje möjlig kant närvarande. Så $K_n = \left([n], \binom{[n]}{2}\right)$, i formell notation.

För en graf G säger vi att ett träd H är ett *uppspännande träd* för G om

- H är en delgraf till G,
- $V_H = V_G$, så varje nod i G är med i H,
- och H är ett träd.



Figur 13: En graf G med kanter i svart och blått. Tar vi enbart de blåa kanterna, och alla noder, får vi en delgraf H som är ett uppspännande träd för G.

Hur många uppspännande träd finns det för K_n?[19]

[19] Ledtråd: Det här är en sak vi redan studerat, bara formulerad på ett annorlunda sätt. Fundera på vad det verkligen betyder att vara ett uppspännande träd för K_n.

Föreläsning 9: Diskret sannolikhetsteori, introduktion · 1MA020

Vilhelm Agdur[1]

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

20 februari 2023

Vi introducerar den diskreta sannolikhetsteorin, vilket är den som behandlar samma sorts objekt som kombinatoriken.

Varför har vi ett avsnitt om diskret sannolikhetsteori[2] i en kurs om kombinatorik?

Diskret sannolikhetsteori och kombinatorik studerar samma klass av objekt – diskreta strukturer – så områdena överlappar. Ofta är vad man ser i början när man lär sig om sannolikhetsteori olika problem vars lösning kan sammanfattas som "översätt till ett problem med att räkna någonting, lös det kombinatorikproblemet, och översätt tillbaka till en sannolikhet".

[2] I kursplanen kallat "klassisk sannolikhetsteori", vilket jag tolkar som en mer tvetydig term för "diskret sannolikhetsteori".

Så det är en anledning till att prata om diskret sannolikhetsteori i denna kurs – vi kan få många exempel, och de exemplen är ofta mer praktiskt tillämpbara än motsvarande kombinatorikproblem. Så när man börjat tröttna på överdrivet abstrakta exempel, eller klämkäcka exempel om glasskiosker, kan sannolikhetsteorin komma som en frisk fläkt.

Men det är så klart inte så att fälten bara överlappar i ena riktningen – det är precis lika sant att det finns många *kombinatoriska* problem där den enklaste och vackraste lösningen använder sannolikhetsteori. Detta kallas för den *probabilistiska metoden*[3] – i dess vanligaste form visar vi att något kombinatoriskt objekt måste existera genom att vi visar att ett slumpmässigt valt objekt kan ha egenskapen. I många fall känner vi inte till något konkret exempel på ett sådant objekt – bara att det måste existera.

[3] På engelska *the probabilistic method* – det finns en utsökt bok med just denna titel av Noga Alon och Joel Spencer som utforskar just detta ämne.

Den lämpar sig definitivt inte som första bok om varken sannolikhetsteori eller kombinatorik, men har man läst någon kurs i vardera ämne och uppnått lite matematisk mognad är den nog ett bra men utmanande val av bok.

Men låt oss börja med att definiera vad vi egentligen menar med diskret sannolikhet.

Händelser och sannolikheter

Definition 1. Ett *sannolikhetsrum* (Ω, μ) består av en mängd Ω och en funktion $\mu : \Omega \to [0,1]$, sådana att

- Ω är icketom och ändlig eller uppräkneligt oändlig[4],
- det gäller att
$$\sum_{\omega \in \Omega} \mu(\omega) = 1.$$

[4] Det vill säga, antingen är den ändlig, eller så kan vi numrera alla dess element $1, 2, 3, \ldots$. Detta är skillnaden mellan diskret och kontinuerlig sannolikhetsteori – i kontinuerlig sannolikhetsteori tillåter vi oss överuppräkneliga mängder.

I den kontinuerliga sannolikhetsteorin behöver man alltså kunna "räkna" saker som är fler än heltalen – det vill säga ta integraler. Som ni kanske är medvetna är det inte helt okomplicerat att definiera vad det ens betyder att ta en integral i allmänhet. Alltså stannar vi i den trevliga diskreta världen, där vi har summor istället för integraler.

Mängden Ω kallas för *utfallsrum*, och elementen ω i Ω alltså för *utfall*.[5] Funktionen μ kallar vi för vårt sannolikhetsmått.

[5] För den som är van med programmering, och vet hur slumpgeneratorer i datorn fungerar, bör man tänka på ω som *seed* till slumpgeneratorn. Det är oftast inte ett intressant objekt i sig, men det bestämmer allt som slumpmässigt händer.

Definition 2. En *händelse* A är en delmängd till Ω. Dess *sannolikhet* ges av

$$\mathbb{P}(A) = \sum_{\Omega \in A} \mu(A).$$

Notera här att vi definierar sannolikheter för *händelser*, **inte för utfall**.[6]

[6] Detta beror på att vi i den kontinuerliga sannolikhetsteorin inte längre kan definiera μ som en funktion från utfall till reella tal, utan måste definiera den som ett genuint *mått*, alltså en funktion från *händelser* (=delmängder) till utfall. Precis som vi inte kan ta integralen av en funktion i en enda punkt, utan tar integraler över intervall.

Ibland kan vi komma att vara slarviga och prata om sannolikheter för enskilda utfall, men det korrekta sättet att skriva är alltid sannolikheten för händelsen $\{\omega\}$, inte för utfallet ω.

Exempel 3. Låt oss formulera de mest uppenbara exemplen av slump i vår nya terminologi.

Vi kan se ett tärningskast som att det har utfallsrum

$$\Omega = \{1, 2, 3, 4, 5, 6\},$$

och sannolikhetsmått μ som skickar varje utfall på $\frac{1}{6}$, alltså $\mu(\omega) = \frac{1}{6}$ för alla ω.

Vad är sannolikheten att vårt tärningskast ger oss ett udda tal? Jo, vad vi frågar efter är sannolikheten för händelsen $U = \{1, 3, 5\}$, vilken vi beräknar som

$$\mathbb{P}(U) = \sum_{\omega \in U} \mu(\omega) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}.$$

Om vi singlar slant har vi istället utfallsrum $\Omega = \{\text{krona}, \text{klave}\}$, och vårt sannolikhetsmått μ är lika med $\frac{1}{2}$ för bägge utfallen.

Sannolikheten att vi får krona är alltså sannolikheten av *händelsen* $\{\text{krona}\}$, och ges av

$$\sum_{\omega \in \{\text{krona}\}} \mu(\omega) = \mu(\text{krona}) = \frac{1}{2}.$$

Vi kan också använda våra kunskaper från tidigare föreläsningar för att lösa mer invecklade problem.

Exempel 4. Antag att en grupp av n stycken försupna studenter går på en efterfest. När festen till slut är över är alla överraskande nog kapabla att gå hem, men ingen är nykter nog att känna igen sin egen jacka, så de bara tar en slumpmässig jacka på vägen ut.

Vad är sannolikheten att *ingen* student kommer hem med sin egen jacka?

Vi får fundera ett ögonblick på hur vi formaliserar det här problemet. Vi kan skriva tilldelningen av jackor till studenter som en permutation av längd n ur alfabetet av jackor.

Om vi numrerar studenterna och jackorna, så att student ett kom dit i jacka ett, student två i jacka två, och så vidare, så kan vi betrakta utfallet som en permutation av $[n]$. Alltså kan vi sätta $\Omega = S_n$, alltså mängden av sådana permutationer.

Hur skall vi tänka för att lista ut vad sannolikheten för varje given permutation är? Vi kan resonera på ett komplicerat sätt med olika

ordningar de kan gå ut i, och varje student tar varje kvarvarande jacka med samma sannolikhet, för att få svaret, eller så kan vi resonera på ett enkelt sätt.

Eftersom alla studenterna är för packade för att kunna se skillnad på jackor är problemet helt symmetriskt – det finns ingen anledning till varför något specifikt utfall skulle vara mer sannolikt än något annat, eftersom studenterna inte kan se skillnad på utfallen oavsett.[7] Alltså måste sannolikheten för varje utfall vara lika, och för att de skall summera till 1 måste de alltså vara $\frac{1}{n!}$.

[7] Jackorna har temporärt gjorts osärskiljbara av övermåga drickande.

Som nästa steg i vår räkning får vi fundera på vad händelsen att ingen student går hem med sin egen jacka är. Det betyder, i vår formulering av utfallen som permutationer av n, att $\omega_i \neq i$ för alla i, alltså att ω är ett derangemang. Så vår händelse är mängden av derangemang, vilka vi ju redan räknat i en tidigare föreläsning att den har storlek

$$n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Så vi kan räkna ut att

$$\begin{aligned}
\mathbb{P}\left(\text{Ingen har sin egen jacka}\right) &= \mathbb{P}\left(\{\omega \in S_n : \omega(i) \neq i \,\forall i\}\right) \\
&= \sum_{\omega \in S_n : \omega(i) \neq i \,\forall i} \mu(\omega) \\
&= \sum_{\omega \in S_n : \omega(i) \neq i \,\forall i} \frac{1}{n!} \\
&= \frac{1}{n!} |\{\omega \in S_n : \omega(i) \neq i \,\forall i\}| \\
&= \frac{1}{n!} n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}
\end{aligned}$$

vilket vi känner igen som de första n termerna i Taylorutvecklingen av e^{-1}, så sannolikheten att ingen får med sig sin egen jacka är, för stora nog n, ungefär 36.8%.

Betingad sannolikhet

Ett av de allra mest användbara verktygen för att resonera om sannolikheter är *betingad sannolikhet*. Det låter oss utföra argument av stilen "under antagandet att A är sant så är sannolikheten för B det här, så eftersom vi vet sannolikheten av A är sannolikheten för B detta". Vi bryter alltså ned ett potentiellt svårt problem i enklare beståndsdelar.

Rent konkret gör vi detta med följande definition:

Definition 5. Givet två händelser A och B, sådana att $\mathbb{P}(B) > 0$, definierar vi *sannolikheten för A givet B* som

$$\mathbb{P}(A \mid B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}.$$

Vi kan tolka detta som att vi "zoomat in" på bara B, och skapat oss ett nytt sannolikhetsmått $\mu_{|B}$, som ges av

$$\mu_{|B} : B \to [0,1] : x \mapsto \frac{\mu(x)}{\sum_{x \in B} \mu(x)}$$

så att

$$\mathbb{P}(A \mid B) = \mu_{|B}(A \cap B).$$

Så termen $\frac{1}{\mathbb{P}(B)} = \frac{1}{\sum_{x \in B} \mu(x)}$ är helt enkelt där för att få sannolikheterna i $\mu_{|B}$ att summera till ett.

Funderar man lite grann på saken bör det kännas rimligt att detta mäter sannolikheten för en händelse, givet att vi redan vet att händelsen B inträffar – vi räknar ju bara på utfallen där B inträffat.

Definition 6. Vi säger att två händelser A och B är *oberoende* ifall

$$\mathbb{P}(A \cap B) = \mathbb{P}(A)\,\mathbb{P}(B).$$

Namnet motiveras av att detta är samma sak som att $\mathbb{P}(A \mid B) = \mathbb{P}(A)$ – att få veta huruvida B inträffade ger oss alltså ingen information alls om ifall A inträffade, vår skattning av sannolikheten för det är helt oförändrad.

Lemma 7 (Lagen om total sannolikhet)**.** *Det är alldeles uppenbart från vår definition att*[8]

$$\mathbb{P}(A \mid B)\,\mathbb{P}(B) = \mathbb{P}(A \cap B).$$

Detta generaliserar enkelt till att, om vi har en samling $B_1, B_2, \ldots B_k$ av disjunkta händelser sådana att

$$A \subseteq \coprod_{i=1}^{k} B_i,$$

alltså sådana att närhelst A inträffar så inträffar exakt en av händelserna B_i, så är

$$\mathbb{P}(A) = \sum_{i=1}^{k} \mathbb{P}(A \mid B_i)\,\mathbb{P}(B_i).$$

I en enkel form får vi alltså för alla *par av händelser A och B att*

$$\mathbb{P}(A) = \mathbb{P}(A \mid B)\,\mathbb{P}(B) + \mathbb{P}(A \mid B^c)\,\mathbb{P}(B).$$

[8] Och som vår diskussion om hur vi använder betingad sannolikhet indikerade är detta den centrala egenskapen den har – den låter oss dela upp det potentiellt svåra problemet att förstå $A \cap B$ i de enklare problemen att förstå B och förstå A givet B.

Exempel 8. Antag att vi har en urna som innehåller hundra glaskulor, som kan vara av glas eller sten, och kan vara antingen röda, gröna, eller blå. Vi drar upp en slumpmässig kula ur vår urna.

Om vi låter A vara händelsen att kulan vi drar är av glas, och B_r, B_g, och B_b vara händelserna att den är *r*öd, *g*rön, eller *b*lå, så säger oss alltså lagen om total sannolikhet att

$$\mathbb{P}(A) = \mathbb{P}(A \mid B_r)\,\mathbb{P}(B_r) + \mathbb{P}\left(A \mid B_g\right)\mathbb{P}\left(B_g\right) + \mathbb{P}(A \mid B_b)\,\mathbb{P}(B_b).$$

Alltså: Om vi vet fördelningen mellan de olika färgerna i urnan (sannolikheterna för B_r, B_g, och B_b) och vi vet hur stor andel av varje given färg som är glaskulor, kan vi räkna ut hur stor andel av alla kulor som är av glas.[9]

[9] Som vi formulerat det här är det ju oerhört oöverraskande att vi kan göra det. Så är det – det är inget märkligt som pågår här. Vad som är överraskande är om något hur ofta lagen om total sannolikhet är användbar, vilket vi kommer se i senare exempel.

Låt oss, innan vi går vidare, ge några basala räkneregler för sannolikheter, som sammanfattning av vad vi sett hittills:

Lemma 9. *Det gäller för alla händelser A och B att*

- *per definition är* $\mathbb{P}(A) = \sum_{\omega \in A} \mu(\omega)$,
- *så* $\mathbb{P}(A^c) = 1 - \mathbb{P}(A)$,
- *och om A och B har tomt snitt, $A \cap B = \emptyset$, så är* $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$,
- *och om de inte nödvändigtvis har tomt snitt har vi att*

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B).$$

- $\mathbb{P}(A \cap B) = \mathbb{P}(A \mid B)\,\mathbb{P}(B)$,
- *och per definition är A och B oberoende precis när* $\mathbb{P}(A \cap B) = \mathbb{P}(A)\,\mathbb{P}(B)$.

Unionsbegränsningar, med tillämpning på Ramseytalen

Vi hade kunnat ge hela detta avsnittet av kursen med enbart exempel om kulor av olika färger i olika urnor – av någon anledning är det det första exemplet som dyker upp i de flesta probabilisters huvud. Låt oss undvika det, och istället ge ett lite mer intressant exempel.

Vi börjar med att påminna oss om ett resultat vi bevisade tidigare, bara omklätt i probabilistisk skrud:

Lemma 10 (Inklusion-exklusion)**.** *Det gäller, för varje samling av händelser $A_1, A_2, \dots, A_n$, att*

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{I \subseteq [n] \\ |I|=k}} \mathbb{P}\left(\bigcap_{i \in I} A_i\right).$$

Så specifikt har vi för varje par av händelser A och B att

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B).$$

Bevis. Vi utelämnar det, eftersom det är så snarlikt till det kombinatoriska fallet vi redan bevisat. □

Låt oss nu introducera ett oerhört potent lemma, som ändock är väldigt enkelt:

Lemma 11 (Unionsbegränsning)**.** *Antag att vi har en samling av händelser $A_1, A_2, \ldots, A_k$. Vi är intresserade av sannolikheten att* någon *av händelserna inträffar, alltså sannolikheten för deras* union*. Det gäller att*

$$\mathbb{P}\left(\bigcup_{i=1}^{k} A_i\right) \leq \sum_{i=1}^{k} \mathbb{P}\left(A_i\right).$$

Bevis. Inklusion-exklusion ger oss att

$$\mathbb{P}\left(\bigcup_{i=1}^{k} A_i\right) = \sum_{i=1}^{k} \mathbb{P}\left(A_i\right) - \left(\sum_{k=2}^{n} (-1)^k \sum_{\substack{I \subseteq [n] \\ |I|=k}} \mathbb{P}\left(\bigcap_{i \in I} A_i\right)\right)$$

och vi kommer ihåg att de extra termerna, som vi stoppat in i ett minustecken, är en korrektion för att vi råkat räkna punkterna i snitten mellan A_i och A_j för många gånger, så alltså måste vi göra höger led större om vi stryker den korrektionen. Alltså har vi vår sökta olikhet. □

Vår första tillämpning är på Ramseytalen, som vi redan sett innan som ett exempel på lådprincipen. Låt oss upprepa vår definition av dessa tal, i en mer rigorös terminologi som vi lärt oss sedan dess.

Definition 12. Tänk att vi tar den fullständiga grafen K_n[10] och målar alla dess kanter antingen röda eller blå.

Ramseytalet $R(k, \ell)$ är det minsta heltalet n sådant att det måste finnas antingen en delmängd av k noder i K_n sådana att alla kanter mellan dem är röda, eller en delmängd av ℓ noder sådana att alla kanter mellan dem är blå. Vi kallar sådana delmängder för *monokromatiska delgrafer*.

[10] Alltså grafen som har n noder, och varje par av noder har en kant mellan dem.

Vi konstaterade när vi först introducerade dessa tal att det är svårt att bevisa saker om dem bortom att de är ändliga, vilket är vad vi gjorde i en övning då. Nu har vi kommit långt nog att vi kan bevisa en faktisk olikhet för dem.

Proposition 13. *Om*

$$\binom{n}{k} 2^{1-\binom{k}{2}} < 1$$

så är $R(k,k) > n$. Således är

$$R(k,k) > \left\lfloor 2^{k/2} \right\rfloor$$

för alla $k \geq 3$.

Bevis. Hur bevisar man att $R(k,k)$ måste vara större än ett visst givet n? Jo, Ramseytalet är ju per definition det minsta n sådant att alla

färgningar av kanterna till K_n har en monokromatisk delgraf av storlek k. Alltså måste vi påvisa någon färgning av kanterna till K_n som inte har en monokromatisk delgraf av någondera färgen.

Det här låter ju som något som kräver en väldigt smart konstruktion. Det stämmer – i själva verket en så smart konstruktion att vi inte faktiskt förmår hitta den.

Det är här den probabilistiska metoden visar sin styrka – vad vi gör istället för att konstruera ett exempel är att välja en *slumpmässig* färgning, och visa att denna har sannolikhet större än noll att ha vår önskade egenskap.

Så, vi tänker oss att vi singlar en slant för varje kant i K_n, där myntets två sidor är "röd" och "blå" – och våra slantsinglingar är oberoende av varandra. Vårt utfallsrum blir då lika med mängden av funktioner från $E(K_n)$, kanter i K_n, till mängden $\{\text{röd}, \text{blå}\}$, där varje blir lika sannolik. Vi kallar våra funktioner ω, och låter alltså $\omega(i,j)$ vara färgen på kanten mellan i och j.

Vad är sannolikheten att vår resulterande graf har en monokrom delgraf av storlek k? Jo, om vi för varje delmängd A till $[n]$ av storlek k låter R_A vara händelsen att A är monokromt röd och B_A vara händelsen att B_A är monokromt blå,[11] så blir händelsen att det finns *någon* monokrom delgraf av den storleken precis[12]

$$\bigcup_{A \in \binom{[n]}{k}} R_A \cup B_A.$$

Hittills verkar det ju inte som att vi gjort några större framsteg – vi har gått från att behöva göra en väldigt smart konstruktion till att behöva förstå en väldigt invecklad mängd av funktioner, som definierats som en union med index i en bunt mängder... Det är här Unionsbegränsningen visar sin kraft, och låter oss lösa ett mycket mycket enklare problem – för om vi tillämpar den så får vi ju att

$$\mathbb{P}\left(\bigcup_{A \in \binom{[n]}{k}} R_A \cup B_A\right) \leq \sum_{A \in \binom{[n]}{k}} \mathbb{P}\left(R_A\right) + \mathbb{P}\left(B_A\right).$$

Vi behöver alltså inte alls förstå oss på den komplicerade unionen, vi behöver bara förstå sannolikheterna för R_A och B_A – och de är mycket enklare, eftersom de ju specificerar precis var den monokroma delgrafen skall finnas: Den skall ligga i A.

Så vad är sannolikheten att just A innehåller enbart röda kanter, alltså sannolikheten för R_A? Jo, den innehåller totalt $\binom{k}{2}$ kanter, och för varje av dessa kanter måste myntet visa den röda sidan. Eftersom våra slantsinglingar är oberoende måste sannolikheten att alla blir röda vara produkten av sannolikheterna för varje mynt att bli rött.

[11] Vill man vara rigorös låter vi alltså

$$R_A = \{\omega : \forall i,j \in A : \omega(i,j) = \text{röd}\}$$

och

$$B_A = \{\omega : \forall i,j \in A : \omega(i,j) = \text{blå}\}.$$

[12] Den här notationen kan vara aningen förvirrande innan man tänkt efter – vi tar en union av en samling mängder, där *index* för summan också är mängder. Men det vi tar unionen över är händelserna $R_A \cup B_A$, inte indexen A.

Alltså tar vi produkten av $\binom{k}{2}$ stycken $1/2$, och får att

$$\mathbb{P}(R_A) = 2^{-\binom{k}{2}}$$

för alla A.

Eftersom problemet är totalt symmetriskt mellan blå och röd gäller samma resultat för B_A, så vi får att

$$\begin{aligned}\sum_{A \in \binom{[n]}{k}} \mathbb{P}(R_A) + \mathbb{P}(B_A) &= \sum_{A \in \binom{[n]}{k}} 2^{1-\binom{k}{2}} \\ &= \binom{n}{k} 2^{1-\binom{k}{2}}\end{aligned}$$

och här kan vi känna igen uttrycket vi antog i formuleringen av satsen var mindre än ett.

Alltså har vi bevisat att sannolikheten att vår slumpmässiga färgning av K_n har en monokromatisk delgraf är mindre än ett – så sannolikheten att den inte har det är större än noll. Men om sannolikheten för detta är större än noll måste det specifikt finnas ett utfall som inte har en monokromatisk delgraf – så vi har hittat vårt exempel på en sådan färgning, helt utan att explicit konstruera det. □

Övningar

Övning 1. Ge ett bevis för Lemma 7.

Övning 2. Visa att

$$\sum_{i=1}^{k} \mathbb{P}(A_i) = \sum_{\omega \in \Omega} |\{i : \omega \in A_i\}| \, \mu(\omega).$$

Använd detta för att ge ett alternativt bevis för Lemma 11.

Övning 3. Vi har n stycken fotbollslag som skall spela i en turnering mot varandra – en väldigt utmattande sådan, eftersom varje lag spelar mot varje annat lag en gång, och oavgjorda matcher avgörs på straffar.

Vi kan tänka oss resultatet av denna turnering som ett sätt att ge varje kant i K_n en *riktning* – kanten pekar från vinnaren till förloraren.

Vi säger att en turnering har *egenskap* S_k om det, för varje samling av k lag, finns ett annat lag som vann mot alla k lagen.

Tänk er nu att dessa alla är amatörlag, som är precis lika usla på fotboll – vinnaren i varje match är helt slumpmässig, och alla matcher är helt oberoende av varandra. Vi helt enkelt singlar en slant för att avgöra vem som vinner.

Deluppgift a: Givet en viss mängd K bestående av k stycken lag, låt A_K vara händelsen att det inte finns något annat lag som slår alla lagen i K. Beräkna $\mathbb{P}(A_K)$.

Deluppgift b: Skriv upp händelsen att vår turnering *inte* har egenskap S_k, i termer av händelserna A_K. Tillämpa en unionsbegränsning på sannolikheten för det här uttrycket, och använd vad ni fick i deluppgift a för att ge ett enkelt uttryck för en övre begränsning på denna sannolikhet.

Deluppgift c: Använd vad ni gjort i tidigare delar av denna uppgift för att ge ett resultat i stil med Proposition 13 om när det finns turneringar med egenskap S_k.

Övning 4. En grupp av sju studenter i en kombinatorikkurs, Anton, Birgitta, Chiara, Damiano, Elisabet, och Francesco[13], är vänner. Totalt är det 35 studenter i klassen.

Deras föreläsare är betydligt elakare än mig, och väljer slumpmässigt ut tre studenter att gå fram och räkna en uppgift vid tavlan.

1. Vad är sannolikheten att Anton blir vald?
2. Vad är sannolikheten att Birgitta blir vald, och de andra två som blir valda inte är med i deras lilla grupp?
3. Vad är sannolikheten att exakt två personer ur vängruppen blir valda?
4. Givet att Francesco blivit vald, vad är sannolikheten att alla tre som valts ut är ur vängruppen?

[13] Det var ovanligt många utbytesstudenter från Italien i just denna klassen.

Övning 5. Antag att du singlar en slant n stycken gånger – men till skillnad från våra vanliga idealiserade mynt är det här myntet lite imperfekt, så sannolikheten att det blir krona ges av p, för något $p \in [0, 1]$.

Vad är sannolikheten att du får precis k stycken krona?[14]

[14] Ledtråd: Betrakta ditt utfallsrum som samlingen av ord av längd n ur alfabetet $\{\text{krona}, \text{klave}\}$. Vad bör $\mu(\omega)$ vara för varje givet ω?

Övning 6 (Svår, frivillig på inlämningsuppgiften)**.** Antag att vi har en samling av händelser $A_1, A_2, \ldots, A_n$, och låt, för varje $1 \leq k \leq n$,

$$\chi_k = \sum_{j=1}^{k} (-1)^{j+1} \sum_{\substack{I \subseteq [n] \\ |I|=j}} \mathbb{P}\left(\bigcap_{i \in I} A_i \right).$$

Alltså blir

$$\chi_1 = \sum_{i=1}^{n} \mathbb{P}\left(A_i\right)$$

och vad vår unionsbegränsning säger är att

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i \right) \leq \chi_1$$

och inklusion-exklusion är påståendet att

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i \right) = \chi_n.$$

Bevisa att vi i allmänhet har att

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) \leq \chi_k$$

för udda k och

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) \geq \chi_k$$

för jämna k.

Föreläsning 10: Slumpvariabler · 1MA020

Vilhelm Agdur[1]

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

27 februari 2023

Vi fortsätter att diskutera diskret sannolikhetsteori, och introducerar slumpvariabler och deras väntevärden.

Vi använder den teori vi byggt upp för att bevisa några fler resultat inom kombinatoriken.

Slumpvariabler

Hittills är vad vi har sett bara hälften av vad man intuitivt tänker ingår i sannolikhetsteorin – vi har diskuterat slumpmässiga *händelser*, som antingen inträffar eller inte, men vi har inte definierat slumpmässiga tal. Frågan om ifall det kommer att regna imorgon eller inte kan vi modellera i vår formalism, men inte frågan om hur många millimeter det kommer regna.

Definition 1. Givet ett sannolikhetsrum (Ω, μ) är en *slumpvariabel* X som tar värden i V en funktion $X : \Omega \to V$. Givet varje utfall tar alltså vår slumpvariabel ett visst värde, och givet varje[2] delmängd $A \subseteq V$ blir $X \in A$ en händelse – specifikt är det händelsen

$$\{\omega \in \Omega \mid X(\omega) \in A\} = X^{-1}(A).$$

[2] Detta är lite av en lögn i det allmänna fallet, eftersom det kan finnas *väldigt* skumma delmängder till V, men så länge vi tänker oss våra diskreta sannolikhetsrum är det sant.

Det allra vanligaste fallet är när $V = \mathbb{R}$ eller någon delmängd till $\mathbb{R}$. I många introtexter om sannolikhetsteori *definierar* man att slumpvariabler tar värden i $\mathbb{R}$ – men eftersom vi sysslar med kombinatorik kommer vi att vilja ha mer exotiska slumpvariabler, som slumpmässiga permutationer eller slumpmässiga mängder.

Exempel 2. Låt oss återbesöka vårt exempel med ett tärningskast. Vi konstaterade att vi kan ta $\Omega = \{1, 2, 3, 4, 5, 6\}$ och $\mu(\omega) = 1/6$ för alla $\omega \in \Omega$.

Vi kan naturligt betrakta vårt tärningskast som en slumpvariabel – i detta fall blir det en mycket enkel funktion, $X : \Omega \hookrightarrow \mathbb{R}$ skickar helt enkelt varje ω på sig självt.

Vårt tärningskast är ett specialfall av ett mer allmänt fenomen, som det kommer vara bekvämt att ha en terminologi för.

Definition 3. Givet en ändlig mängd V är ett *likformigt fördelat slumpmässigt element av* V en slumpvariabel X sådan att $\mathbb{P}(X = v) = \frac{1}{|V|}$ för varje $v \in V$.[3] Alla element av V är alltså lika sannolika. Vi kan skriva detta som

$$X \overset{\text{u}}{\in} V.$$

[3] Vill man göra detta fullständigt rigoröst i vår formalism kan man säga att X är definierad på sannolikhetsrummet (V, μ) där $\mu(v) = \frac{1}{|V|}$ för alla $v \in V$, och $X : V \to V$ är identitetsfunktionen.

Men det blir väldigt många abstrakta ord för att inte säga så mycket alls som vi inte redan sade när vi definierade X som att den blir lika med varje element i V med samma sannolikhet.

Detta innebär alltså att för varje mängd $W \subseteq V$ så blir

$$\mathbb{P}(X \in W) = \frac{|W|}{|V|}.$$

Om någon säger att "vi låter X vara en slumpmässig graf / träd / mängd / etc." utan att specificera hur X är fördelad menar de att den är likformig.

Vi vet att om vi slår vår tärning många gånger kommer vi i genomsnitt att få upp 3.5. Hur gör vi den intuitionen rigorös?

Definition 4. *Väntevärdet* av en slumpvariabel X som tar värden i $\mathbb{R}$ ges av[4]

$$\mathbb{E}[X] = \sum_{x \in X(\Omega)} x\mathbb{P}(X = x).$$

Vi tar alltså summan över alla tänkbara värden x för X, multiplicerar x med sannolikheten att X faktiskt blir x,[5] och summerar. I specialfallet där X bara tar värden $0, 1, 2, \ldots$ blir alltså formeln

$$\mathbb{E}[X] = \sum_{k=0}^{\infty} k\mathbb{P}(X = k).$$

Exempel 5. Så om vi åter tar exemplet med tärningskastet så blir alltså väntevärdet

$$\begin{aligned}\mathbb{E}[X] &= 1\mathbb{P}(X=1) + 2\mathbb{P}(X=2) + \ldots + 6\mathbb{P}(X=6) \\ &= \frac{1+2+3+4+5+6}{6} = \frac{7}{3} = 3.5\end{aligned}$$

precis som vi förväntade oss.

Ibland är det mer användbart att skriva definitionen av väntevärde på en alternativ form:

Lemma 6. *Det gäller att*[6]

$$\mathbb{E}[X] = \sum_{\omega \in \Omega} X(\omega)\mu(\omega).$$

Bevis. Vi kan skriva

$$\begin{aligned}\mathbb{E}[X] &= \sum_{x \in X(\Omega)} x\mathbb{P}(X = x) \\ &= \sum_{x \in X(\Omega)} x \left(\sum_{\omega \in \Omega : X(\omega) = x} \mu(\omega) \right) \\ &= \sum_{x \in X(\Omega)} \sum_{\omega \in \Omega : X(\omega) = x} x\mu(\omega) \\ &= \sum_{x \in X(\Omega)} \sum_{\omega \in \Omega : X(\omega) = x} X(\omega)\mu(\omega) \\ &= \sum_{\omega \in \Omega} X(\omega)\mu(\omega).\end{aligned}$$

□

[4] Notera att detta är en summa över *alla värden som X kan tänkas ta* – eftersom vi antagit att Ω är ändligt eller uppräkneligt så kommer detta vara en summa över ändligt eller uppräkneligt många summander, vilket är okej.

Hade vi velat modellera en *kontinuerlig* slumpvariabel – som till exempel en normalfördelning, som nog många sett redan – som kan ta vilket reellt tal som helst som värde, hade vi behövt definiera detta som en integral, inte en summa. Att slippa ge definitioner som fungerar i dessa fall är en av anledningarna till varför vi begränsar oss till bara diskret sannolikhetsteori.

[5] Notera att när den här summan löper över oändligt många tal är det fullt möjligt att den inte konvergerar, trots att $\sum_{x \in X(\Omega)} \mathbb{P}(x = X) = 1$. Det finns slumpvariabler som alltid tar ändliga värden, men ändå har oändligt väntevärde.

[6] Det här fungerar bara för att vi har antagit att våra sannolikhetsrum är ändliga eller uppräkneligt oändliga, så vi kan skriva våra sannolikheter som summor. I det mer allmänna fallet hade vi behövt skriva en integral mot sannolikhetsmåttet, och det kräver betydligt mer avancerad analys än vad vi kan.

Eftersom vi definierat slumpvariabler som att de helt enkelt är funktioner från Ω kan vi göra all den algebra vi vanligen kan på funktioner in i $\mathbb{R}$. Till exempel är det, givet två slumpvariabler X och Y, helt väldefinierat att skriva $X + Y$, och det betyder precis vad vi förväntar oss att det skall betyda – vi slumpar ett X och ett Y och sedan adderar vi dem med varandra.

När vi nu har introducerat addition av slumpvariabler så kan vi bevisa vad som, i min mening, är en av de allra mest användbara satserna i hela matematiken.[7]

[7] Jag är så klart oerhört partisk, eftersom just gränslandet mellan kombinatorik och sannolikhetsteori är mitt område – men det är onekligen ett otroligt användbart resultat.

Lemma 7 (Väntevärdets linjäritet)**.** *Givet två slumpvariabler X och Y och två reella tal a och b gäller det att*

$$\mathbb{E}\left[aX + bY\right] = a\mathbb{E}\left[X\right] + b\mathbb{E}\left[Y\right].$$

Väntevärdet är alltså linjärt, som funktion från rummet av slumpvariabler in i $\mathbb{R}$.[8]

[8] Detta sätt att formulera det skrapar lite på ytan av en väldigt djup teori – väntevärden är nämligen "bara" integraler mot sannolikhetsmått, och samlingen av funktioner från Ω in i $\mathbb{R}$ blir ju ett vektorrum. Vi kan ge det vektorrummet en inre produkt genom att skriva $\langle X, Y\rangle = \mathbb{E}\left[XY\right]$, och vi har börjat med funktionalanalys.

Men detta är ju en kurs i kombinatorik, så att utforska detta får vänta till en framtida kurs för er.

Bevis. Vi använder den alternativa formeln för väntevärde vi fann i Lemma 6 och skriver

$$\begin{aligned}\mathbb{E}\left[aX + bY\right] &= \sum_{\omega\in\Omega} (aX + bY)(\omega)\mu(\omega)\\ &= \sum_{\omega\in\Omega} (aX(\omega) + bY(\omega))\mu(\omega)\\ &= a\sum_{\omega\in\Omega} X(\omega)\mu(\omega) + b\sum_{\omega\in\Omega} Y(\omega)\mu(\omega)\\ &= a\mathbb{E}\left[X\right] + b\mathbb{E}\left[Y\right].\end{aligned}$$

□

För att göra det här verkligt användbart behöver vi konceptet med indikatorvariabler, som vi introducerade när vi bevisade inklusion-exklusion.

Proposition 8. *För en händelse A blir dess indikatorfunktion $\mathbb{1}_A$, som ges av att $\mathbb{1}_A(\omega) = 1$ om $\omega \in A$ och noll annars, en slumpvariabel.*[9]

[9] Det är ju en funktion från utfall till reella tal – per definition är det en slumpvariabel. Vi behöver bara känna igen att den är det.

Det gäller att

$$\mathbb{P}\left(A\right) = \mathbb{E}\left[\mathbb{1}_A\right].$$

Bevis. Per definition har vi att

$$\begin{aligned}\mathbb{E}\left[\mathbb{1}_A\right] &= 0\cdot\mathbb{P}\left(\mathbb{1}_A = 0\right) + 1\cdot\mathbb{P}\left(\mathbb{1}_A = 1\right)\\ &= \sum_{\omega:\mathbb{1}_A(\omega)=1} \mu(\omega)\\ &= \sum_{\omega\in A} \mu(\omega) = \mathbb{P}\left(A\right).\end{aligned}$$

□

Sperners lemma

Låt oss nu ta vad vi har lärt oss och tillämpa det på ett faktiskt kombinatoriskt resultat.

Definition 9. En samling $\mathcal{F}$ av delmängder till $[n]$ kallas för en *anti-kedja* ifall det för varje par $F, G \in \mathcal{F}$ varken gäller att $F \subset G$ eller $G \subset F$.

Hur stor kan en anti-kedja vara? Ett enkelt sätt att skapa sig en sådan är att ta alla delmängder av storlek k till $[n]$ för något k. Att dessa inte kan vara delmängder till varandra är uppenbart. Att det val av k som gör denna anti-kedja som störst blir $\lfloor \frac{n}{2} \rfloor$ är inte allt för svårt att se.[10] Är det möjligt att hitta en ännu större genom att ha med delmängder av olika storlekar? Sperners lemma säger oss att svaret är nej.

[10] Vi hade också kunnat välja $\lceil \frac{n}{2} \rceil$, det ger samma storlek.

Lemma 10 (Sperners lemma)**.** *För varje anti-kedja $\mathcal{F}$ i $[n]$ gäller det att*

$$|\mathcal{F}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

Bevis. Vi tar en likformigt slumpmässig permutation σ av $[n]$, och låter I vara mängden av i sådana att

$$\{\sigma(1), \sigma(2), \ldots, \sigma(i)\} \in \mathcal{F}.$$

Det är enkelt att se att I innehåller antingen noll eller ett element – om den innehöll både i och j, med $i < j$, vore ju

$$\{\sigma(1), \sigma(2), \ldots, \sigma(i)\} \subset \{\sigma(1), \sigma(2), \ldots, \sigma(i), \sigma(i+1), \ldots, \sigma(j)\},$$

vilket skulle motsäga att $\mathcal{F}$ är en antikedja.

Låt oss nu studera slumpvariabeln $X = |I|$. Att vi vet att I bara kan ha noll eller ett element ger oss omedelbart att $\mathbb{E}[X] \leq 1$,[11] men låt oss studera detta väntevärde också på ett annat sätt.

Vi kan räkna att[12]

$$\begin{aligned}\mathbb{E}[X] = \mathbb{E}[|I|] &= \mathbb{E}\left[\sum_{i=1}^{n} \mathbb{1}_{\{i \in I\}}\right] \\ &= \sum_{i=1}^{n} \mathbb{E}\left[\mathbb{1}_{\{i \in I\}}\right] = \sum_{i=1}^{n} \mathbb{P}(i \in I).\end{aligned}$$

Vad är sannolikheten att i ligger i I? Att i ligger i I betyder att $\{\sigma(1), \sigma(2), \ldots, \sigma(i)\} \in \mathcal{F}$, per definition. Så vad vi behöver förstå är den slumpmässiga *mängden*

$$U_i = \{\sigma(1), \sigma(2), \ldots, \sigma(i)\}.$$

[11] Detta kan vi göra till ett allmänt lemma:

Lemma 11. *Om $X(\omega) \leq C$ för varje $\omega \in \Omega$ gäller det att $\mathbb{E}[X] \leq C$.*

Bevis. Vi kan räkna

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

□

[12] Här använder vi den kortare notationen $\mathbb{1}_{\{i \in I\}}$ för att beteckna $\mathbb{1}_{\{\omega \in \Omega : i \in I(\omega)\}}$.

Eftersom vi valde σ som en slumpmässig permutation finns det ingen anledning till varför något tal skulle vara mer sannolikt än något annat att dyka upp i denna mängd. U_i är alltså, av symmetriskäl, ett likformigt slumpmässigt element ur $\binom{[n]}{i}$, mängden av delmängder av storlek i.

Vad är sannolikheten att U_i faller i $\mathcal{F}$? Jo, om vi låter $\mathcal{F}_i$ beteckna samlingen av element i $\mathcal{F}$ av storlek i vet vi att $\mathcal{F}_i \subseteq \binom{[n]}{i}$ och $U_i \overset{u}{\in} \binom{[n]}{i}$, så vi måste ha att

$$\mathbb{P}\left(U_i \in \mathcal{F}_i\right) = \frac{|\mathcal{F}_i|}{\binom{n}{i}}.$$

Så samlar vi ihop vad vi har listat ut hittills i ett enda uttryck, och använder olikheten[13] $\binom{n}{\lfloor \frac{n}{2} \rfloor} \geq \binom{n}{i}$ för alla i, har vi att

$$1 \geq \mathbb{E}\left[X\right] = \sum_{i=1}^{n} \mathbb{P}\left(i \in I\right) = \sum_{i=1}^{n} \frac{|\mathcal{F}_i|}{\binom{n}{i}} \geq \sum_{i=1}^{n} \frac{|\mathcal{F}_i|}{\binom{n}{\lfloor \frac{n}{2} \rfloor}}$$

så multiplicerar vi bägge sidorna av detta med $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ får vi att

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} \geq \sum_{i=1}^{n} |\mathcal{F}_i| = |\mathcal{F}|$$

vilket är precis Sperners lemma, som vi ville bevisa. □

[13] Vi har strikt sett inte faktiskt bevisat den någon gång, men det bör vara någorlunda enkelt att övertyga sig själv om att den är sann.

Caro-Weis sats

Antag att vi har en grupp av n personer på ett läger, och säg att person nummer i känner d_i andra personer sedan tidigare. Du vill bilda en mindre grupp av personer för en lära-känna-varandra-lek[14], så du vill hitta en så stor grupp som möjligt av personer som *inte* känner varandra. Finns det någon garanti för hur stor du kan göra den mindre gruppen?

[14] Eftersom du är en fruktansvärt ondskefull person. Ingen tycker om sådana lekar.

Teorem 12 (Caro-Wei)**.** *Du kan välja den mindre gruppen sådan att den har åtminstone*

$$\sum_{i=1}^{n} \frac{1}{d_i + 1}$$

medlemmar.

Eller formulerat i mer matematiska termer: Varje graf G på n noder, där nod i har grad d_i[15]*, har alltid en oberoende mängd*[16] *S sådan att*

$$|S| \geq \sum_{i=1}^{n} \frac{1}{d_i + 1}.$$

Bevis. Numrera noderna i G från 1 till n, och välj sedan likformigt slumpmässigt ett nytt sätt att etikettera G, så att nod i nu har etikett $\sigma(i)$. σ är alltså en likformig permutation av $[n]$.

[15] Ett ord vi inte har definierat, som får en definition i sidnoterna:

Definition 13. *Graden* av en nod v i en graf $G = (V_G, E_G)$ är antalet kanter som går ut från v. Alltså

$$d_v = |e \in E_G \mid v \in e|.$$

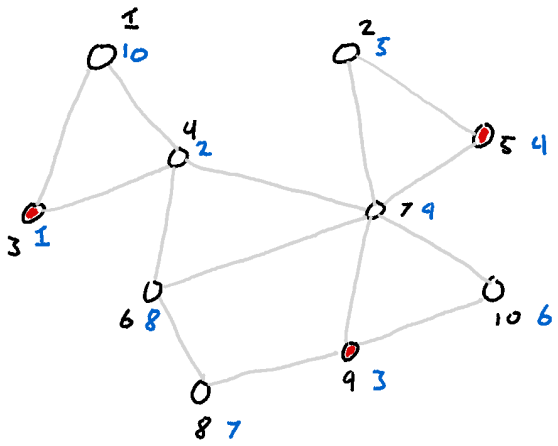
[16] Nästa hitintills odefinierade term, och nästa sidnot:

Definition 14. En *oberoende mängd* $S \subseteq V_G$ i en graf $G = (V_G, E_G)$ är en mängd av noder sådana att det inte finns några kanter mellan något par av noder i S. Alltså, mängden

$$E(S) = \{\{u, v\} \in E_G \mid u, v \in S\}$$

är tom.

Hur använder vi detta för att skapa vår oberoende mängd? Jo, beteckna mängden av grannar till i med $N(i)$ – alltså mängden av alla noder som har en kant till i. Om vi lägger in i i S får vi alltså inte ta med något annat element i $N(i)$ om S skall vara en oberoende mängd.[17]



Figur 1: En illustration av vår konstruktion av den oberoende mängden S. Vår första etikettering av grafen är i svart, vår ometikettering σ i blått, och den resulterande oberoende mängden S markerad i rött.

Om vi nu låter

$$S = \{i \in V_G \mid \sigma(i) < \sigma(j) \quad \forall j \in N(i)\}$$

så hävdar vi att detta måste vara en oberoende mängd. Varför? Tänk för motsägelse att det fanns ett par i, j i S med en kant mellan sig. Eftersom i ligger i S måste alla is grannar ha högre etikett än i – specifikt så måste alltså $\sigma(i) < \sigma(j)$. Men det betyder ju att j har en granne med lägre etikett, så j kan inte ligga i S, och vi har en motsägelse.

Vi vill alltså förstå oss på mängden S. Låt A_i vara händelsen att i fick en lägre etikett än alla sina grannar i vår slumpmässiga ometikettering – vi har då av väntevärdets linjäritet att

$$\mathbb{E}\left[|S|\right] = \mathbb{E}\left[\sum_{i=1}^{n} \mathbb{1}_{A_i}\right] = \sum_{i=1}^{n} \mathbb{P}\left(A_i\right).$$

Det räcker alltså för oss att förstå sannolikheterna för händelserna A_i. Eftersom σ var likformigt slumpmässig betyder det alltså att vi vill räkna antalet sätt att etikettera grafen sådana att i får en lägre etikett än alla sina grannar.

För att konstruera ett sådant sätt att etikettera G börjar vi med att välja vilka tal som skall stå på i och dess grannar – detta kan vi göra på $\binom{n}{d_i+1}$ sätt, eftersom vi skall ha d_i etiketter på dess grannar och en etikett på den själv.

Sedan väljer vi hur vi placerar dessa etiketter på d_i och $N(i)$ –

[17] Tänk er det som att vi lägger ett pussel, där varje bit är "formad som" en $N(i)$, och vi inte får lov att välja två pusselbitar som överlappar. Målet är att lyckas lägga så många bitar som möjligt. (Det här går nog att omvandla till ett faktiskt spel – jag kräver inga royalties för idén.)

vi måste så klart välja att placera det lägsta av talen på i, men de återstående d_i talen kan vi placera ut fritt[18], och alltså på $d_i!$ sätt.

Till slut väljer vi hur vi placerar resten av etiketterna på noderna utanför is grannskap – detta kan vi också göra helt fritt, så på $(n - d_i - 1)!$ sätt. Så totalt har vi sett att det finns

$$\binom{n}{d_i + 1} d_i!(n - d_i - 1)!$$

sätt att välja en etikettering av G sådan att i får en lägre etikett än alla sina grannar.

Så sannolikheten att en slumpmässig etikettering är sådan ges alltså av

$$\begin{aligned}\mathbb{P}(A_i) &= \frac{1}{n!}\binom{n}{d_i+1} d_i!(n-d_i-1)! \\ &= \frac{1}{n!}\frac{n!}{(d_i+1)!(n-(d_i+1))!} d_i!(n-d_i-1)! \\ &= \frac{1}{d_i+1}\end{aligned}$$

så

$$\mathbb{E}[|S|] = \sum_{i=1}^{n} \mathbb{P}(A_i) = \sum_{i=1}^{n} \frac{1}{d_i+1}.$$

Vi har alltså visat att vi *i genomsnitt* hittar en oberoende mängd av vår sökta storlek med denna metoden. Men det genomsnittliga utfallet kan ju omöjligen vara mindre än *alla* specifika utfall[19] – alltså måste det finnas något specifikt val av σ sådant att storleken på $S(\sigma)$ blir åtminstone detta. Alltså är vi klara. □

Första-moment-metoden

Hittills har vi sett ett sätt som väntevärden och sannolikheter kan samspela – om slumpvariabeln vi vill studera kan formuleras som antalet "ja" på en samling ja-nej-frågor så får vi att dess väntevärde är summan av sannolikheterna för ett "ja" på varje enskild fråga.

Detta låter oss alltså svara på en fråga om ett väntevärde genom att räkna ut en bunt sannolikheter. Hur gör vi om det vi verkligen är intresserade av är en sannolikhet?

Lemma 16 (Markovs olikhet)**.** *Om en icke-negativ[20] slumpvariabel X har väntevärde ν gäller det för varje $C > 0$ att[21]*

$$\mathbb{P}(X > C\nu) < \frac{1}{C}.$$

Bevis. Vi kan räkna att[22]

[18] Det är här som vår teknik med väntevärdets linjäritet verkligen lönar sig – vi har kunnat zooma in bara på i, och behöver inte bry oss om vad som händer utanför just i. Hade vi inte gjort det hade vi kanske behövt bekymra oss om kanter mellan is grannar här, och inte kunnat placera ut etiketterna helt fritt.

[19] Låt oss formulera detta som ett lemma och bevisa det:

Lemma 15. *För varje slumpvariabel X med $\mathbb{E}[X] = C$ måste det finnas åtminstone ett ω sådant att $X(\omega) \geq C$.*

Bevis. Antag för motsägelse att $X(\omega) < C$ för alla ω. Då kan vi räkna att

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

så $C < C$, en motsägelse. □

[20] Det vill säga, $X(\omega) \geq 0$ för alla $\omega \in \Omega$ – den tar aldrig ett negativt värde.

[21] Eller ekvivalent att

$$\mathbb{P}(X > C) \leq \frac{\nu}{C}.$$

[22] Var i beviset använder vi antagandet att X är ickenegativ?

$$\begin{aligned}\nu = \mathbb{E}[X] &= \sum_{\omega\in\Omega} X(\omega)\mu(\omega) \\ &\geq \sum_{\substack{\omega\in\Omega \\ X(\Omega)>C\nu}} X(\omega)\mu(\omega) \\ &> \sum_{\substack{\omega\in\Omega \\ X(\Omega)>C\nu}} C\nu\mu(\omega) \\ &= C\nu\mathbb{P}(X > C\nu)\end{aligned}$$

så om vi delar bägge sidor av detta med $C\nu$ får vi resultatet. □

Vad för slags problem kan man tänkas tillämpa det här verktyget på?

Definition 17. En Erdős-Renyi-graf (med parametrar n och p) är en slumpmässig graf G på n noder, där varje kant är med med sannolikhet p, oberoende av om varje annan kant är med. Vi skriver att $G \sim G_{n,p}$.

Om $p = \frac{1}{2}$ så kommer alltså $G_{n,p}$ helt enkelt vara en likformigt slumpmässig graf på n noder, men för det mesta kommer vi vara intresserade av fallet när p är en funktion av n.

Vi kan säga en hel del om den "lokala" strukturen av en $G_{n,p}$ bara med de verktyg vi har lärt oss hittills – alltså de egenskaper hos den som vi kan avgöra om de gäller genom att studera den lokalt runt varje nod. Desto svårare blir det om vi ställer oss frågor om ifall den är, till exempel, sammanhängande.

Ett exempel på en lokal struktur är ifall vi har isolerade noder – om vi tänker oss det som att noderna är personer och kanterna är vänskapsrelationer är vi alltså intresserade av sannolikheten att inte ha några vänner.[23]

[23] Som vi alla vet går denna upp markant om man studerar matematik, men vår modell är inte sofistikerad nog att fånga detta.

Proposition 18. *Om $p > \frac{c\log(n)}{n}$ för något $c > 1$ så finns det asymptotiskt nästan säkert*[24] *inga isolerade noder*[25] *i $G_{n,p}$.*

[24] Vad sjutton betyder det? Det betyder att, om p_n är en följd sådan att $p_n > \frac{\log(n)}{n}$ för varje n, och G_n är en G_{n,p_n} för varje n, så går sannolikheten att G_n har en isolerad nod mot noll.

[25] Och vad är en isolerad nod? Det är en nod utan grannar.

Bevis. Beviset följer ett mönster som förhoppningsvis börjar bli bekant vid det här laget.

Låt $G \sim G_{n,p}$. Vi låter I_i vara händelsen att nod i är isolerad, och konstaterar att om I är mängden av isolerade noder i G så är

$$\mathbb{E}[|I|] = \sum_{i=1}^{n} \mathbb{P}(I_i)$$

så vad vi behöver räkna ut är sannolikheten att en viss given nod är isolerad.

Detta är en relativt enkel beräkning – det finns $n-1$ noder som i hade kunnat ha en kant till, och varje kant finns med sannolikhet p,

oberoende av varje annan kant. Alltså är sannolikheten att inga av kanterna finns $(1-p)^{n-1}$, och vi har att

$$\mathbb{E}\left[|I|\right] = \sum_{i=1}^{n} \mathbb{P}\left(I_i\right) = n(1-p)^{n-1}$$

och Markovs olikhet ger oss nu, för varje $C > 0$, att

$$\mathbb{P}\left(|I| > C\nu\right) < \frac{1}{C}. \tag{1}$$

Hur omvandlar vi detta till det resultat vi vill ha? Om vi tar ett väldigt litet ϵ och låter $C = \frac{1-\epsilon}{\nu}$ så blir (1) till

$$\mathbb{P}\left(|I| > 1-\epsilon\right) < \frac{\nu}{1-\epsilon}.$$

Eftersom $|I|$ självklart enbart tar heltalsvärden är händelsen i vänster led precis samma händelse som händelsen att $|I| \geq 1$, det vill säga $I \neq \emptyset$.[26] Så om vi ersätter vänster led med detta får vi att

$$\mathbb{P}\left(I \neq \emptyset\right) < \frac{\nu}{1-\epsilon}$$

och här kan vi utan problem ta gränsvärdet $\epsilon \to 0$ och få[27]

$$\mathbb{P}\left(I \neq \emptyset\right) \leq \nu.$$

Så det enda som återstår att göra är att visa att ν går mot noll. Enligt satsens antaganden har vi att $p > c\frac{\log(n)}{n}$, så vi kan räkna att

$$\begin{aligned}
\lim_{n\to\infty} \nu &= \lim_{n\to\infty} n(1-p)^{n-1} \\
&\leq \lim_{n\to\infty} n\left(1 - c\frac{\log(n)}{n}\right)^{n-1} \\
&= \lim_{n\to\infty} \frac{n}{1-c\frac{\log(n)}{n}}\left(1 - \frac{c\log(n)}{n}\right)^{n} \\
&= \lim_{n\to\infty} n \underbrace{\frac{1}{1-c\frac{\log(n)}{n}}}_{\to 1 \text{ när } n\to\infty} \left(\underbrace{\left(1 - \frac{c}{n/\log(n)}\right)^{\frac{n}{\log(n)}}}_{\to e^{-c} \text{ när } n\to\infty}\right)^{\log(n)} \\
&= \lim_{n\to\infty} n\left(e^{-c}\right)^{\log(n)} = \lim_{n\to\infty} n^{1-c}
\end{aligned}$$

och eftersom $c > 1$ går detta mot noll, såsom önskat.[28] □

Det finns några saker som är värda att anmärka på här. Om vi hade valt $c \leq 1$ hade inte vår räkning fungerat längre – och detta är inte ett sammanträffande eller ett resultat av att vi använde en svag metod.

[26] Varje tänkbart värde på $|I|$ som är större än $1-\epsilon$ är också ≥ 1, och vice versa.

[27] Notera att vi, när vi tar gränsvärdet här, måste ersätta $<$ med $\leq$ – för oss är det inget problem eftersom vi oavsett skall visa att ν går mot noll.

[28] I steget mellan rad fyra och fem går vi väldigt snabbt fram – egentligen hade man behövt kolla att

$$f(n,c) = \left(1 - \frac{c}{n/\log(n)}\right)^{\frac{n}{\log(n)}}$$

går mot e^{-c} snabbt nog att vi får lov att göra den substitutionen. Som tur är gäller det att $f(n,c) - e^{-c}$ är ungefär $\frac{\log(n)}{n}$ – specifikt

$$\frac{e^{-c} - f(n,c)}{\frac{\log(n)}{n}} \to \frac{c^2}{2e^c}$$

vilket är bra nog. Men detta är mycket mer analys än vad vi faktiskt vill göra i denna kurs.

I själva verket kan man visa att antalet isolerade noder faktiskt kommer gå mot oändligheten om $p < \frac{\log(n)}{n}$ – så vårt resultat är det bästa möjliga.

Vi nämnde innan att vi kan studera lokala problem som dessa enkelt, men att "globala" problem är svårare, och nämnde frågan om grafen är sammanhängande som ett exempel på en svår global fråga. I själva verket kan man visa att grafen kommer vara sammanhängande så snart vi inte längre har några isolerade noder – så detta resultat tillsammans med vad vi just visade visar alltså att en Erdős-Renyi-graf är sammanhängande så snart $p \geq \frac{c\log(n)}{n}$.

Räkneregler för slumpvariabler

Vi sammanfattar vad vi lärt oss om slumpvariabler hittills i följande räkneregler:[29]

[29] Den här biten skippar vi på föreläsningen – den ligger här för att vara behjälplig som sammanfattning och när man gör övningarna. Den finns också i vår samling av formler och räkneregler.

Lemma 19. *Om (Ω, μ) är något sannolikhetsrum, $A \subseteq \Omega$ någon händelse, och $X, Y : \Omega \to \mathbb{R}$ samt $Z : \Omega \to V$ är slumpvariabler som tar värden i $\mathbb{R}$ och i någon godtycklig mängd V, så gäller att:*

1. $$\mathbb{E}[X] = \sum_{x \in X(\Omega)} x\mathbb{P}(X = x) = \sum_{\omega \in \Omega} X(\omega)\mu(\omega).$$

2. *För alla $a, b \in \mathbb{R}$ så är*

   $$\mathbb{E}[aX + bY] = a\mathbb{E}[X] + b\mathbb{E}[Y].$$

   Väntevärdet är alltså en linjär funktional.

3. $$\mathbb{P}(A) = \mathbb{E}[\mathbb{1}_A].$$

4. *Om $X(\omega) \leq C$ för varje ω, eller ekvivalent om $\mathbb{P}(X \leq C) = 1$, så är $\mathbb{E}[X] \leq C$.*

5. *Om $\mathbb{E}[X] = C$ så finns det åtminstone ett ω sådant att $X(\omega) \geq C$.*

6. *Markovs olikhet ger oss att, om $\mathbb{E}[X_n] \to 0$ för någon följd av ickenegativa slumpvariabler X_n som enbart tar heltalsvärden, så måste också $\mathbb{P}(X_n > 0) \to 0$.*

7. *Om Z är likformigt fördelad på V så gäller det för varje delmängd $W \subseteq V$ att*

   $$\mathbb{P}(Z \in W) = \frac{|W|}{|V|}.$$

Övningar

Övning 1.

Definition 20. En familj $\mathcal{F}$ av delmängder till $[n]$ kallas för *skärande* om $A \cap B \neq \emptyset$ för alla par av A och B i $\mathcal{F}$.

Hur stor kan en skärande familj av mängder vara, om vi kräver att varje $A \in \mathcal{F}$ har storlek exakt k? Svaret ges av följande sats:

Teorem 21 (Erdős-Ko-Rado)**.** *För varje skärande familj $\mathcal{F}$ av delmängder av storlek k till $[n]$ gäller det att*

$$|F| \leq \binom{n-1}{k-1}.$$

Delfråga a: Hitta, för alla n och k, ett exempel på en skärande familj $\mathcal{F}$ av delmängder av storlek k till $[n]$ sådan att

$$|F| \leq \binom{n-1}{k-1}.$$

Delfråga b: Bevisa följande lemma:[30]

[30] Den här delen kräver ingen probabilistisk metod, det är bara ett direkt bevis. Sannolikhetsteorin kommer in i nästa delfråga.

Lemma 22. *Låt $\mathcal{F} \subseteq \binom{[n]}{k}$ vara en skärande familj, och låt för varje $s \in \{0, 1, \ldots, n-1\}$*

$$A_s = \{s, s+1, \ldots, s+k-1\}$$

där additionen är modulo n. Då kan $\mathcal{F}$ innehålla högst k av mängderna A_s.

Dra sedan slutsatsen från detta att samma lemma gäller även om vi tar någon permutation $\sigma \in S_n$ och låter

$$A_s = \{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\}.$$

Delfråga c: Nu skall vi bevisa Erdős-Ko-Rado. Idén är att vi vill skapa en likformigt slumpmässig $A \overset{u}{\in} \binom{[n]}{k}$ och studera sannolikheten att denna ligger i $\mathcal{F}$ – det finns ett uppenbart uttryck för denna sannolikhet, och vi vill skapa A på ett sätt som gör att vi också kan använda vårt lemma från förra delfrågan för att begränsa den.

Beviset börjar alltså med "Tag en likformigt fördelad permutation $\sigma \overset{u}{\in} S_n$ och ett likformigt fördelat heltal $s \overset{u}{\in} \{0, 1, \ldots, n-1\}$". Skriv resten av beviset.

Övning 2. Bevisa följande proposition:

Proposition 23. *Antag att $v_1, v_2, \ldots, v_n$ är n stycken enhetsvektorer i $\mathbb{R}^n$, alltså $\|v_i\| = 1$ för alla i. Då finns det en följd $\eta_1, \eta_2, \ldots, \eta_n$, med $\eta_i = \pm 1$ för varje i, sådan att*

$$\left\| \sum_{i=1}^{n} \eta_i v_i \right\| \leq \sqrt{n}.$$

Övning 3. I denna övning skall vi bevisa följande resultat:

Teorem 24. *Låt $G = (V, E)$ vara någon graf, och antag att $|V| = n$ och $|E| = n\frac{d}{2}$ för något $d \geq 1$. Då finns det en oberoende mängd i G av storlek åtminstone $\frac{n}{2d}$.*

Idén för beviset är att vi tar en slumpmässig delmängd $S \subseteq V$ genom att ta med varje nod med sannolikhet $p = \frac{1}{d}$. Denna kommer så klart inte vara garanterad att vara en oberoende mängd – men om vi, för varje kant $\{u, v\}$ som kopplar ihop $u, v \in S$, tar bort u eller v ur S så blir den återstående mängden av noder oberoende.

Bevisa satsen genom att räkna ut väntevärdet av storleken på S och väntevärdet av antalet noder vi tvingas ta bort ur S, och se att vi kommer ha i genomsnitt $\frac{n}{2d}$ noder kvar.

Övning 4. Låt $p \in (0, 1)$ vara fixt. För varje $i \in \mathbb{N}$, låt

$$X_i = \begin{cases} 1 & \text{med sannolikhet } p \\ 0 & \text{annars,} \end{cases}$$

så att $X_1, X_2, X_3, \ldots$ blir en slumpmässig följd av nollor och ettor. Låt I vara det minsta I sådant att $X_I = 0$ – detta blir alltså ett slumpmässigt heltal.

Beräkna, för varje $i \in \mathbb{N}$, $\mathbb{P}(I = i)$. Räkna sedan ut $\mathbb{E}[I]$.

Övning 5. Antag att du samlar på Pokemonkort.[31] Vi föreställer oss en väldigt enkel modell för hur du får ett nytt kort – det finns n stycken distinkta kort totalt, och du kan köpa ett nytt kort åt taget. Det nya kortet du får är likformigt fördelat i samlingen av kort – varje kort är lika sannolikt.

När du köper ditt första kort är du garanterad att få ett kort du inte har innan. När du köper ditt andra kort är sannolikheten bara $\frac{1}{n}$ att du råkar få det kort du redan fick en gång – men när du redan har de flesta av korten kommer du oftast bara att få ett kort du redan äger, inte ett nytt, så du behöver köpa väldigt många paket för att gå från att ha en samling av $n - 1$ kort till att ha en fullständig samling.

Låt T vara antalet gånger du behöver köpa ett nytt kort för att få en fullständig samling, om du börjar på noll. Beräkna $\mathbb{E}[T]$.[32]

[31] Ersätt med ditt favorit-gacha med lootboxes om du vill ha ett mer samtida exempel.

[32] Ledtråd: Lösningen på det här problemet använder lösningen på föregående problem.

Föreläsning 11: Probabilistiska metoden · 1MA020

Vilhelm Agdur[1]

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

11 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.

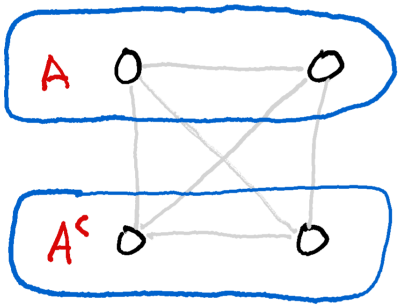
För att kunna göra snabba beräkningar vill vi alltså hitta ett sätt att dela upp vår graf så att det inte går så många kanter mellan de två delarna. Det här är ett problem som behöver lösas i praktiken, även om man ofta då har fler än två datorer och behöver hitta en minimal k-partition av grafen istället.

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.

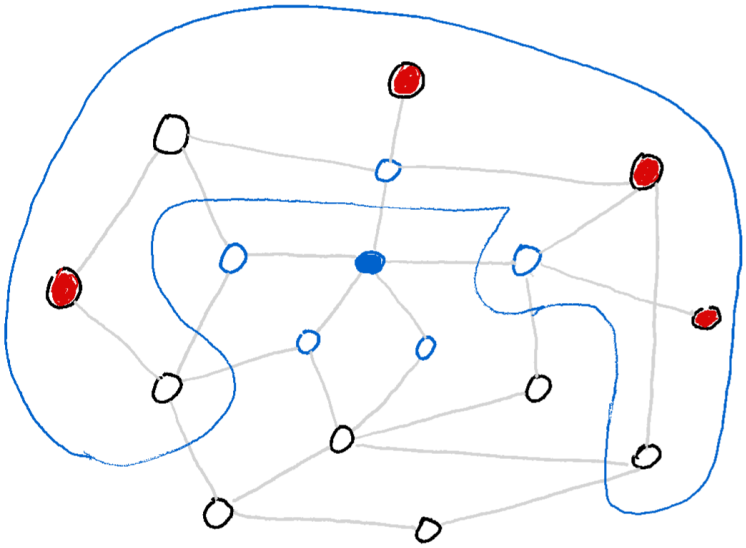
I vänster led skrev vi en betingad sannolikhet där vi betingade på en *slumpvariabel*, men vi har ju definierat betingade sannolikheter som att vi betingar på *händelser*.

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.

Sammanfattning av hela kursen · 1MA020

Vilhelm Agdur[1]

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

11 mars 2023

Detta dokument ger en sammanfattning av kursens innehåll, med nyckelord markerade, och saker vi räknat eller bevisat.

Kursen är uppdelad i tre delar – vi började med grundläggande kombinatorik i de första fyra föreläsningarna, sedan introducerade vi genererande funktioner i de kommande tre föreläsningarna. Sedan hade vi ett intermezzo om grafer och träd i en föreläsning, innan vi fortsatte till vår tredje del om diskret sannolikhetsteori och den probabilistiska metoden.

Del ett: Grundläggande kombinatorik

I den första föreläsningen introducerade vi de allra mest grundläggande koncepten i kombinatoriken:

1. Additionsprincipen och multiplikationsprincipen låter oss räkna olika mängder.
2. Ord bildade ur olika alfabeten är det mest basala av alla kombinatoriska objekt.
3. Ett viktigt exempel på en slags ord är permutationer – vi definierar och räknar dessa.
4. Om ord är det mest basala exemplet där ordning spelar roll är kombinationer det mest grundläggande exemplet på när vi väljer saker utan ordning.
5. Vi definierar binomialkoefficienterna och visar att dessa räknar antalet kombinationer av en viss storlek.

Precis i slutet av föreläsning ett börjar vi prata om kombinatoriska bevis. I föreläsning två fortsätter vi på detta tema, och ger ett antal olika exempel.

1. De flesta av våra kombinatoriska bevis involverar binomialkoefficienter, alltså delmängder till en viss mängd i en kombinatorisk tolkning.
2. Vi bevisar specifikt binomialsatsen med ett kombinatoriskt bevis.
3. Sedan definierar vi omordningar och använder dessa för att räkna multi-delmängder[2] med ett pinnar-och-stjärnor-argument.

[2] Just termen multi-delmängd introducerar vi tyvärr först i en senare föreläsning – i efterhand borde termen ha dykt upp redan här. Den refererar till ett sätt att fördela ut n osärskiljbara objekt till k särskiljbara personer, om vi inte kräver att varje person måste få ett objekt.

4. Vi ser vårt första exempel av att räkna lösningar till ekvationer när vi tolkar en multi-delmängd som en lösning på en ekvation $x_1 + x_2 + \ldots + x_n = k$ – detta kommer dyka upp igen senare i kursen, med fler begränsningar på vad variablerna kan ta för värden.

5. Vi definierar multinomialkoefficienterna, och ser att dessa ger antalet omordningar av ett ord.

I den tredje föreläsningen i denna del av kursen introducerar vi några till enkla verktyg inom kombinatoriken.

1. Lådprincipen, i dess generaliserade form, låter oss visa en del överraskande resultat. Vi ger ett par enkla exempel, och ett lite mer sofistikerat.

2. Inklusion-exklusion låter oss räkna många saker som annars vore väldigt svåra att räkna. För att kunna bevisa den introducerar vi indikatorfunktioner och ger några räkneregler för dessa.

3. Vi använder inklusion-exklusion för att räkna lösningar till ekvationer, nu med övre begränsningar på variablerna.

4. Vi definierar derangemang, och använder inklusion-exklusion för att räkna dessa.

Föreläsning fyra sammanfattar till slut vad vi gjort i denna del av kursen.

1. Vi definierar Stirlings partitionstal, och använder inklusion-exklusion för att visa att antalet surjektioner från en mängd till en annan räknas av en formel som involverar dessa.

2. Vi definierar mängdpartitioner och visar att dessa räknas av Stirlings partitionstal. Dessa ger oss ett till vanligt exempel på något vi kan ge kombinatoriska bevis kring.

3. Vi skriver upp en stor tre-gånger-fyra tabell över många av de räkneproblem vi sysslat med hittills – den tolvfaldiga vägen – som sammanfattar och systematiserar det hela i termer av särskiljbara och osärskiljbara objekt och funktioner som kan vara generella, injektiva, eller surjektiva.

4. Vi definierar Stirlings cykeltal, och därmed också cykler i permutationer. Vi visar hur man kan omvandla mellan en permutation i vanlig form och en i cykelform.

Del två: Genererande funktioner

I den här delen av kursen introducerar vi ett mer mekaniskt maskineri än tidigare – innan var våra metoder ofta skräddarsydda för problemen, men genererande funktioner ger ofta ett generellt recept på en lösning.

Första föreläsningen, föreläsning fem totalt, lade grunderna,

1. gav definitionen av en (ordinär) genererande funktion,
2. räknade ut vad genererande funktionen var för några enkla exempel,
3. och använde vår metod för att hitta genererande funktionen för Fibonaccitalen.
4. Mer allmänt såg vi hur man kan manipulera summor för att omvandla rekursioner för följder till ekvationer för deras genererande funktioner, och lösa dessa för att få ut den genererande funktionen.
5. Sedan definierade vi faltningen av två följder, och bevisade att den genererande funktionen för faltningen av två följder är produkten av deras genererande funktioner.
6. Vi använde detta för att räkna lösningar till ekvationer med begränsningar på variablerna[3] – eller i alla fall hitta genererande funktionen för antalet lösningar, vilket oftast är gott nog.
7. Vi utnyttjade också algebraiska manipulationer för genererande funktioner för att bevisa likheter mellan olika följder eller hitta genererande funktionen för en följd.[4]

Andra föreläsningen om genererande funktioner, föreläsning sex totalt, fortsatte på samma tema, med mer räkning av lösningar till ekvationer. Sedan

1. såg vi ett exempel på hur man kan finna en rekursion för ett kombinatoriskt problem,
2. definierade exponentiella genererande funktioner och
3. fann några exempel på sådana för olika följder.
4. Sedan återvände vi till rekursionen vi funnit tidigare, och såg hur vi kan finna en differentialekvation för den exponentiella genererande funktionen för en följd givet en rekursion. Att faktiskt lösa differentialekvationen är oftast möjligt, men inte riktigt en del av denna kursen, som ju inte handlar om analys.

[3] I biten om multidelmängder kunde vi ha begränsningar av typen $x_4 \geq 72$, sedan när vi använde inklusion-exklusion kunde vi ha mer generella begränsningar av typen $3 \leq x_2 \leq 14$. När vi använder genererande funktioner kan vi ha mycket mer generella begränsningar, som till exempel på pariteten till x_7.

[4] Detta dyker inte upp fullt så mycket i själva föreläsningen, men övning tre och fyra i föreläsningsanteckningarna är bra exempel på principen.

5. Sedan definierade vi binomialfaltningen mellan två följder, och visade att den exponentiella genererande funktionen för binomialfaltningen mellan två följder är produkten av deras genererande funktioner.

6. Vi använde sedan detta för att räkna antalet ord ur olika alfabeten, under olika begränsningar på antalet av en viss bokstav – och såg att det var helt analogt med hur vi räknade lösningar på ekvationer.

I tredje föreläsningen om genererande funktioner, föreläsning sju totalt, genomförde vi en mer omfattande räkning med genererande funktioner. Vi

1. definierade gitterstigar, uppåt-höger-stigar, och Dyckstigar.

2. Sedan fann vi en rekursion, Segner-rekursionen, för antalet Dyckstigar,

3. och använde denna för att hitta genererande funktionen för antalet Dyck-stigar.

4. Sedan definierade vi den stigande och fallande fakulteten, och använde dessa med Newtons binomialsats för att ge ett omständligt men helt mekaniskt bevis för vår explicita formel för Catalantalen.

5. Efter det gav vi ett kombinatoriskt bevis för samma formel, som helt skippade att behöva hitta en rekursion och genererande funktion.

6. Vi gav några fler exempel på saker som räknas av Catalantalen, och visade att de faktiskt räknas av dem genom att visa att de lyder Segner-rekursionen.[5]

[5] För att vara tydlig: Det intressanta här är inte nödvändigtvis de specifika exemplen, även om de är nyttiga, utan att allmänt förstå hur vi, genom att visa att ett objekt kan delas upp i två mindre objekt av samma typ, kan visa att någon följd lyder Segnerrekursionen och alltså räknas av Catalantalen.

Intermezzo: Grafer och träd

I vår åttonde föreläsning hade vi ett litet intermezzo, där vi introducerade några koncept som behövs för framtiden. Specifikt

1. definierade vi grafer, som kan vara etiketterade eller ej,

2. och träd (alltså sammanhängande grafer utan cykler), som kan vara ordnade eller oordnade, och ha eller inte ha en rot.

3. Vi definierade vad vi menar med binära träd, och visade att de rotade ordnade binära oetiketterade träden med n interna noder räknas av Catalantalen, eftersom dessa lyder Segner-rekursionen.

4. Sedan visade vi att de rotade ordnade oetiketterade träden på $n+1$ noder också räknas av Catalantalen, genom att ge en bijektion mellan dessa och parentetiseringar av uttryck.

5. Sedan introducerade vi Cayleys formel. För att motivera den räknade vi etiketterade träd – specifikt, givet ett oetiketterat träd, räknade vi antalet sätt att sätta en etikett på det.
6. Vi gav sedan vårt första bevis av Cayleys formel med hjälp av Prüferkoder. Vi såg hur man finner Prüferkoden för ett träd, och gav en algoritm för att konstruera ett träd givet en Prüferkod.
7. Efter det ville vi ge ett alternativt bevis av Cayleys formel, och för detta behövde vi introducera ett par nya koncept, nämligen vad det betyder för en graf att vara en delgraf till en annan, vad en riktad graf är för något, och vad en skog är.
8. Sedan gav vi vårt alternativa bevis för Cayleys formel.

Del tre: Diskret sannolikhetsteori och den probabilistiska metoden

I denna del av kursen introducerade vi den andra större metoden inom kombinatoriken som vår kurs täcker – den probabilistiska metoden. För att kunna göra detta behövde vi så klart först introducera vårt verktyg, den diskreta sannolikhetsteorin.

Denna delen innehåller många olika exempel och satser – ingen av dem är enskilt central, men att se den övergripande metoden, den röda tråden, är det. Alltså är inte själva satserna markerade, men metoderna kan vara det.

I den första föreläsningen, nummer nio totalt, så

1. definierade vi sannolikhetsrum bestående av utfallsrum och sannolikhetsmått,
2. och kallade delmängder till utfallsrummet för händelser, och definierade sannolikheten för händelser.
3. Vi gav några enkla exempel på hur man kan beskriva problem i denna formalism – och efter det var vi så vaga vi kunde komma undan med om hur exakt problemen formaliseras i den.[6]
4. Vi definierade den betingade sannolikheten, vad det betyder att händelser är oberoende, och formulerade lagen om total sannolikhet.
5. Sedan formulerade vi inklusion-exklusion i dess sannolikhetsteoretiska version, och använde denna för att bevisa unionsbegränsningen.
6. Vi använde unionsbegränsningen för att bevisa en undre begränsning för Ramseytalen. Vi gjorde detta genom att välja en slumpmässig färgning och räkna på sannolikheten för att delgrafer skulle bli monokromatiska.

[6] Detta var inte bara att jag var lat – det är en universell standard bland sannolikhetsteoretiker att sopa det under mattan som irrelevanta detaljer. Man måste kunna definitionerna, men i nittionio fall av hundra behöver man inte tänka så noga på dem.

I föreläsning två i denna del, nummer tio totalt,

1. definierade vi slumpvariabler, och specialfallet med likformiga slumpvariabler.
2. Sedan definierade vi väntevärdet av en slumpvariabel, och bevisade ett lemma som gav en alternativ formel för väntevärdet.
3. Vi bevisade sedan väntevärdets linjäritet, och fann en koppling mellan väntevärdet av indikatorvariabeln för en händelse och sannolikheten för denna händelse.
4. Vi använde sedan detta för att bevisa Sperners lemma och Caro-Weis sats. I bägge fallen involverade idén att välja en slumpmässig permutation, och använda den för att skapa ett nyttigt objekt – en slumpmässig kedja i Sperners lemma, och en slumpmässig oberoende mängd för Caro-Wei – som vi sedan kunde studera för att få fram resultatet.
5. Vi bevisade sedan Markovs olikhet, och definierade Erdős-Renyi-grafer,
6. och bevisade ett villkor för när Erdős-Renyi-grafen inte har några isolerade noder. Idén var helt enkelt att räkna ut väntevärdet av antalet isolerade noder, med hjälp av väntevärdets linjäritet, och sedan använda Markovs olikhet för att se att det faktum att detta väntevärde gick mot noll gav att sannolikheten att det existerade isolerade noder också gick mot noll.

Föreläsning tre i denna del, den elfte och sista i kursen, introducerade nästan inga nya koncept, utan gav bara ytterligare exempel på hur man kan använda den probabilistiska metoden.

1. Vi började med att bevisa en nedre begränsning för `min-bisection`. Vi gjorde detta genom att utnyttja Diracs sats för att hitta en Hamiltoncykel i komplementgrafen, tog varannan kant i den cykeln för att få en matchning disjunkt från kanterna i grafen, och valde sedan hälften av noderna som vårt A genom att ta en ur varje par.
2. Sedan visade vi ett resultat av Ajtai-Chvatal-Newborn-Szemerédi-Leighton om det minimala antalet korsningar mellan kanter i en ritning av en graf. Idén var att ta en känd olikhet för detta, och tillämpa den på en slumpmässig delgraf där vi behöll varje nod med en viss sannolikhet. Eftersom detta skalade antalet noder, antalet kanter, och antalet korsningar på olika sätt[7] kunde vi få ut en bättre olikhet av detta.
3. Till slut bevisade vi ett till resultat om oberoende mängder, nu i triangelfria grafer, efter en bevisidé av Shearer. Till skillnad från vår

[7] Snarlikt till hur man, om man halverar sidlängden på en kub, minskar dess yta till en fjärdedel och dess volym till en åttondel.

vanliga procedur där vi tog en enkelt slumpfördelning och byggde objektet vi var ute efter, tog vi här direkt en slumpmässig oberoende mängd, och ansträngde oss för att förstå hur den betedde sig.