Kimmo Eriksson
Matematiska institutionen, SU

12 december 1995

Att genomföra och formulera ett bevis

Att lösa uppgifter av karaktären "Bevisa att..." uppfattas av många studenter som svårt. Ofta är det inte så svårt egentligen, om man bara tillåter sig att inse vad som ska verifieras. Men även om man tror sig om att kunna genomföra beviset så kan man råka ut för att det sedan underkänns av examinatorn (om man går en kurs) eller refereen (om man skickat resultatet till en tidskrift) för att man inte har formulerat det ordentligt. I den här i en hast hopkomna skriften tänkte jag försöka ge er råd om hur man bevisar saker och ge träning i att formulera bevisen. Allt är färgat av min kombinatoriska personliga läggning.

Att formulera bevis.

Det finns fyra grundregler för bevisföring som man bör påminna sig.

1. Ett bevis ska bryta ned ett komplicerat resonemang i delar som är så enkla att de inte behöver ifrågasättas!
2. Bevisbördan ligger på den som bevisar!
3. Alla satsens förutsättningar bör dyka upp i beviset!
4. Man får aldrig anta det som ska bevisas!

Ett bevis ska bryta ned ett komplicerat resonemang i delar som är så enkla att de inte behöver ifrågasättas!

Idealet är ju *modus ponens*: Om A är sant och det är sant att $A \Rightarrow B$ så är också B sant. Man vill komma ned till så enkla byggstenar av typen A och $A \Rightarrow B$ att de inte kräver vidare verifikation.

Exempel. SATS: Chansen att få exakt tio rätt på tipset på en godtycklig rad är $\binom{13}{3}2^3/3^{13}$.

BEVIS: Chansen att få exakt tio rätt på tipset på en godtycklig rad, givet en viss korrekt rad, är (antalet rader som skiljer sig från den rätta på exakt tre matcher) delat med (det totala antalet möjliga rader man kan tippa). Att välja ut tre matcher av tretton kan göras på $\binom{13}{3}$ sätt, och för var och en av dem ska vi välja något av de två felaktiga resultaten så det blir 2^3 möjligheter. Totalt finns alltså $\binom{13}{3}2^3$ rader som skiljer sig från den rätta på exakt tre matcher. Det totala antalet möjliga rader man kan tippa är 3^{13}, ty det finns tre möjligheter för var och en av de tretton matcherna.

Ju högre matematisk nivå på läsaren av beviset, desto större munsbitar kan man anta att hon kan förstå på en gång. Men så fort man utan verifikation presenterar ett påstående som läsaren inte inser sanningshalten i så har man misslyckats.

Bevisbördan ligger på den som bevisar!

Ibland invänder läsaren av ett bevis att "det där är väl inget bevis". Då är det antagligen inte det. Ett riktigt bevis ska inte lämna utrymme för invändningar.

Exempel. SATS: Man kan inte välja ut sex rektangulära papperslappar med längd och bredd heltal mellan ett och tio så att ingen lapp täcker någon annan lapp.

BEVISFÖRSÖK: Välj först lapp $(10, 1)$ med längd tio och bredd ett. Den täcker alla andra av bredd ett. Välj nästa lapp $(9, 2)$. Den täcker alla andra av bredd två utom $(10, 2)$ som ju täcker $(10, 1)$ och alltså inte får väljas. På samma sätt väljer vi $(8, 3)$, $(7, 4)$ och $(6, 5)$. Vi kan nu inte välja ut någon sjätte lapp som inte täcks av någon vald eller täcker någon vald.

INVÄNDNING: — Men det här visar ju bara att om man väljer sina lappar just *så här* så kan man inte välja någon sjätte. Det skulle ju mycket väl kunna finnas något annat val av fem lappar som medgav en sjätte lapp.

OJUST MOTINVÄNDNING: — Jaså? Hur skulle det se ut?

Det är inte den som läser beviset som ska styrka sina invändningar genom att hitta ett motexempel. Om satsen är sann, som i exemplet, finns ju inget motexempel. Nej, det är den som bevisar som ska ge ett heltäckande argument så att inga invändningar återstår.

Alla förutsättningar till satsen bör tydligt användas i beviset!

Satser brukar se ut som "Om *förutsättningar* så *slutsats*". I beviset vill man då se tydligt hur var och en av förutsättningarna kommer in i beviset. Antagligen är ju förutsättningarna nödvändiga för att slutsatsen ska vara sann, så om någon förutsättning inte verkar användas i beviset är det troligt att beviset är fel.

Exempel. I en sammanhängande, plan graf, låt v, e och r var antalet hörn, kanter och regioner. Visa att $v - e + r = 2$.

BEVISFÖRSÖK: Det gäller för ennodsgrafen: $v = 1$, $e = 0$, $r = 1$. Induktion. Anta att påståendet är sant för alla grafer som är mindre än G. Vi ska visa att det måste vara sant för G. Antingen är G ett träd, och då har det ett löv x. Påståendet är då sant för $G - x$ som har en nod och en kant färre men samma antal regioner, och är därmed sant även för G. Eller också har G en cykel, som innehåller någon kant f. Påståendet är då sant för $G - f$ som har en kant färre och en region färre (två regioner smälte samman till en när f togs bort), och är därmed sant för G.

Förutsättningen att grafen skulle vara sammanhängande, vart tog den vägen? Det ser ut som om vi bevisar att $v - e + r = 2$ för alla plana grafer, men påståendet är ju falskt för alla icke sammanhängande plana grafer. I beviset borde vi hänvisat till sammanhängandet när vi påstod att G antingen måste vara ett träd eller ha en cykel, och vi skulle också ha påpekat att $G - x$ och $G - f$ blev sammanhängande för att kunna använda induktionshypotesen — som naturligtvis också måste innehålla förutsättningen.

Man får aldrig anta det som ska bevisas!

Säg att man ska bevisa t ex att $D(n) = n(D(n-1) + D(n-2))$ och att det första man skriver i beviset är $D(n) = n(D(n-1) + D(n-2))$. Då är man redan förlorad! Att anta motsatsen och visa att det leder till en motsägelse är en just bevisteknik, men att anta satsen och konstatera att man därmed kan härleda något som är sant visar tyvärr inte att satsen är sann.

Problemtyper och bevistyper

Olika sorters påståenden kräver olika sorters bevis. Jag tänker ta upp följande sätt att bevisa ett påstående:

1. Verifiera enligt definitioner.
2. Dela upp i uttömmande fall.
3. Anta motsatsen och finn motsägelse.
4. Induktion över någon parameter.
5. Kontraposition: Om A ska medföra B kan man lika gärna bevisa att icke B medför icke A.
6. Bevisa identiteter via bijektion.
7. Bevisa att något kan uppnås genom att visa att man alltid kan ta ett steg närmare.

Verifiera enligt definitioner

När man får i uppgift att bevisa ett påstående så är det första och viktigaste steget att *precis förstå* vad det det faktiskt är man ska bevisa. Man ska alltså tränga in i definitionerna av alla förekommande begrepp. Har man väl gjort det känns ofta satsen självklar, så att man inte ens förstår vad man ska skriva i beviset. Men i så fall är det just detta man ska skriva ner, nedbrytandet av påståendet i mer grundläggande begrepp där beviset blir en ren verifikation.

Exempel. En sammanhängande graf är *2-sammanhängande* om man måste ta bort minst två noder för att den inte längre ska vara sammanhängande. Två stigar mellan x och y är *noddisjunkta* om de inte har någon nod gemensam (mer än x och y). Visa att en graf G är tvåsammanhängande om det finns minst två noddisjunkta stigar mellan varje par av noder som inte är grannar.

BEVIS: Om det finns två noddisjunkta stigar mellan varje par av noder som inte är grannar så finns det minst en stig kvar om man tar bort en nod vilken som helst. Att två noder är grannar påverkas inte av att en annan nod tas bort. Alltså, om man tar bort en nod x vilken som helst från G finns fortfarande en stig mellan varje par av noder i $G - x$ vilket ekvivalent med att $G - x$ är sammanhängande. Alltså måste man ta bort minst två noder från G för att grafen inte längre ska vara sammanhängande. Med andra ord är G 2-sammanhängande.

Dela upp i uttömmande fall

Ett svåröverblickbart problem kan ofta delas upp i flera separata fall som kan behandlas var för sig. Det viktiga här är att det är tydligt att det inte kan finnas fler fall, dvs att man verkligen uttömt alla möjligheter. Kempes berömda felaktiga bevis för fyrfärgssatsen hade just detta fel; han hade inte tänkt på att det fanns ytterligare ett fall att behandla.

Exempel. Varje graf $G = (V, E)$ är förstås isomorf med sig själv, med identitetsisomorfin $f(x) = x$ för alla hörn x i V. En graf har *icketrivial automorfi* om den har ytterligare någon isomorfi med sig själv. Visa att varje träd som inte har någon icketrivial automorfi och som har fler än ett hörn faktiskt måste ha minst sju hörn.

BEVIS: Anta att trädet T inte har någon icketrivial automorfi. Ett träd är antingen en stig eller också finns något hörn x av grad minst tre. Varje stig x_0–x_1–$\cdots$–x_n har uppenbarligen en icketrivial automorfi: $f(x_i) = x_{n-i}$ för alla hörn x_i. Alltså är T ingen stig utan har något hörn x av grad minst tre, dvs det går ut minst tre grenar från x. Om två av grenarna bara består av ett hörn, y_1 resp y_2, så finns uppenbarligen en icketrivial automorfi: $f(y_1) = y_2$, $f(y_2) = y_1$, och $f(y) = y$ för alla andra hörn y. Alltså kan högst en gren i T ha ett enda hörn. Om två av grenarna består av precis två hörn, y_1–y_2 och y_3–y_4, så finns uppenbarligen en icketrivial automorfi: $f(y_1) = y_3$, $f(y_2) = y_4$, $f(y_3) = y_1$, $f(y_4) = y_2$, och $f(y) = y$ för alla andra hörn y. Alltså kan högst en gren i T ha precis två hörn. Alltså har T minst sju hörn: x och dess minst tre grenar vilka som minst består av ett, två respektive tre hörn.

Anta motsatsen och finn motsägelse

Om man vill bevisa att en sats är sann kan man anta att den är falsk och visa att det leder fram till en motsägelse. Nedanstående berömda motsägelsebevis fanns av Euklides för tvåtusen år sedan.

Exempel. Ett *primtal* kan definieras som ett heltal större än ett som inte delas av något mindre primtal. Visa att det finns oändligt många primtal.

BEVIS: Anta motsatsen, att det bara finns ändligt många primtal, nämligen $p_1, p_2, \ldots, p_k$. Bilda det större talet $M = p_1 p_2 \cdots p_k + 1$. Det är klart att M inte delas av något av talen $p_1, p_2, \ldots, p_k$ och eftersom de enligt antagandet är alla primtal så delas inte M av något mindre primtal och är därmed själv ett primtal. Men det motsäger antagandet det bara fanns primtalen $p_1, p_2, \ldots, p_k$, som alltså måste vara falskt.

Induktion över någon parameter

Induktionsbevis bygger på att man kan formulera påståendet över någon parameter $n \geq n_0$. Om man kan visa dels att påståendet är sant i basfallet $n = n_0$ och dels att det är sant för $n = k + 1$ om man antar att det är sant för $n = k \geq n_0$, ja då har man visat det för alla $n \geq n_0$.

Exempel. Låt G vara en bipartit graf G med nodmängd $X \cup Y$ där alla noder har grad n. Visa att G har n stycken kantdisjunkta kompletta matchningar.

BEVIS: Påståendet är uppenbarligen sant för $n = 0$. Anta att det är sant för $n = k$ och låt G vara en bipartit graf där alla noder har grad $n = k+1$. Låt A vara en godtycklig delmängd till X. Antalet kanter från A måste vara högst lika med antalet kanter till bilden $R(A)$, dvs $n \cdot |A| \leq n \cdot |R(A)|$. Alltså är $|A| \leq |R(A)|$ för varje $A \subseteq X$, så enligt Halls sats finns en komplett matchning. Ta bort kanterna i denna matchning. Då försvinner precis en kant från varje nod, så i den återstående grafen har varje nod grad k och enligt induktionsantagandet finns alltså k kantdisjunkta matchningar. Tillsammans med den borttagna finns alltså $k + 1 = n$ kantdisjunkta matchningar i G.

Kontraposition

Kontraposition innebär att man i stället för att bevisa påståendet "A medför B" visar det ekvivalenta påståendet "icke B medför icke A". Denna omtolkning gör man ofta helt automatiskt och behöver inte påpekas.

Exempel. Givet ett träd T, visa att det finns exakt en stig mellan varje par av noder i T.

BEVIS: Anta att det finns något par av noder i T som inte har exakt en stig mellan sig. Antingen har de då noll stigar mellan sig, men då är T inte sammanhängande och är därmed inget träd. Eller också finns det minst två stigar mellan detta par av noder, med då har T en cykel och är därmed inget träd.

Bevisa steg för steg

Om man ska visa att det går att uppnå en viss situation kan man göra det genom att visa att man från varje annan situation kan komma ett steg närmare den önskade situationen. En variant på det här är om man ska bevisa att en viss medlem L i en familj är optimal i något avseende. Då räcker det att visa att man från varje annan medlem i familjen kan komma ett steg närmare L i ett steg som inte försämrar, men eventuellt förbättrar.

Exempel. Givet positiva tal $x_1 \leq x_2 \leq \cdots \leq x_n$ och $y_1 \leq y_2 \leq \cdots \leq y_n$, betrakta produktsummorna $x_1 y_{\pi(1)} + x_2 y_{\pi(2)} + \cdots + x_n y_{\pi(n)}$ för alla tänkbara permutationer π. Visa att den största är $x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$, dvs när π är identitetspermutationen: $\pi(i) = i$ för alla i.

BEVIS: I varje permutation π som inte är identitetspermutationen finns ett par närliggande tal som kommer i fel ordning: $\pi(i) > \pi(i+1)$. Vi ska visa att man inte minskar produktsummans värde om man sorterar detta par rätt, dvs vi ska visa att $x_i y_{\pi(i)} + x_{i+1} y_{\pi(i+1)} \leq x_i y_{\pi(i+1)} + x_{i+1} y_{\pi(i)}$. Det följer av att differensen mellan högerledet och vänsterledet är

$$x_i y_{\pi(i+1)} + x_{i+1} y_{\pi(i)} - (x_i y_{\pi(i)} + x_{i+1} y_{\pi(i+1)}) = (x_{i+1} - x_i)(y_{\pi(i)} - y_{\pi(i)})$$

som är ickenegativt eftersom båda faktorerna är ickenegativa. Från varje produktsumma kan vi alltså sortera om par som kommer i fel ordning utan att minska produktsumman, men eventuellt öka den. Alltså får vi den största summan för den helt sorterade permutationen.

Bevisa identiteter via bijektion

Numeriska identiteter, dvs att ett visst antal är lika med ett visst annat antal, kan ofta bevisas med ren formell manipulation. Ibland är det enklare eller åtminstone vackrare att bevisa identiteten genom att presentera en bijektion mellan en mängd vars antal är vänsterledet och en annan mängd vars antal är högerledet. Ett sådant bevis kallas *kombinatoriskt* eller helt enkelt *bijektivt*. Helst ska bijektionen vara så enkel att man inser att det är en bijektion så fort man ser den.

Exempel. Visa att antalet heltalspartitioner av $2n$ i jämna delar är lika med antalet heltalspartitioner av n i godtyckliga delar.

BEVIS: Vi ska definiera en bijektion f från mängden av partitioner av $2n$ i jämna delar till mängden av partitioner av n i godtyckliga delar. Varje partition av $2n$ i jämna delar kan skrivas som $(2x_1, 2x_2, \ldots, 2x_k)$ där $x_1 \geq x_2 \geq \cdots \geq x_k$ och $x_1+x_2+\ldots+x_k = n$. Definiera $f(2x_1, 2x_2, \ldots, 2x_k) = (x_1, x_2, \ldots, x_k)$. Det är uppenbarligen en injektiv och surjektiv funktion till mängden av partitioner av n i godtyckliga delar.

Uppgifter

Här kommer nu ett par bevis som är felaktiga, trots att satserna är korrekta. Er uppgift är att inse varför dessa bevis är felaktiga!

1. SATS: *Det kromatiska polynomet $P(G, \lambda)$ för en graf G med n stycken hörn är ett polynom $\lambda^n - a_{n-1}\lambda^{n-1} + a_{n-2}\lambda^{n-2} - a_{n-3}\lambda^{n-3} + \ldots$ där alla a_i är ickenegativa heltal, dvs koefficienterna har alternerande tecken.*

   BEVIS: Induktion. Sant för grafen med ett hörn, ty den har kromatiskt polynom λ. Anta bevisat för grafer med upp till $n-1$ hörn. Låt x vara något hörn i G. Då är $P(G-x, \lambda)$ på formen $\lambda^{n-1} - a'_{n-2}\lambda^{n-2} + a'_{n-3}\lambda^{n-3} - a'_{n-4}\lambda^{n-4} + \ldots$, och x kan sedan färgas med någon av $\lambda - r$ färger, där r är antalet olika färger som används på x:s grannar. Alltså är $P(G, \lambda) = P(G-x, \lambda) \cdot (\lambda - r) =$

   $$\lambda^n - (r + a'_{n-2})\lambda^{n-1} + (ra'_{n-2} + a'_{n-3})\lambda^{n-2} - (ra'_{n-3} + a'_{n-4})\lambda^{n-3} + \ldots$$

   vilket är på önskad form.

2. SATS: *Det finns oändligt många primtal på formen $4n+1$.*

   BEVIS: Anta motsatsen, att det bara finns ändligt många primtal på denna form, nämligen $p_1, p_2, \ldots, p_k$. Bilda det större talet

   $$M = 4p_1p_2 \cdots p_k + 1.$$

   Talet M är på formen $4n+1$ och det har inget av primtalen $p_1, p_2, \ldots, p_k$ som faktor, och är alltså självt ett primtal, vilket motsäger antagandet.

Och nedan följer en del uppgifter där det gäller att formulera bevis så noggrant som möjligt.

1. Bevisa att antalet delmängder av $\{1, 2, \ldots, n\}$ som har jämnt antal element är lika med antalet delmängder av $\{1, 2, \ldots, n\}$ som har udda antal element.

   Tips! Para ihop varje mängd som innehåller elementet 1 med motsvarande mängd där just elementet 1 är borttaget.

2. Visa att det finns oändligt många primtal på formen $4n+3$ där n är heltal.

   Tips! Varje udda tal är antingen på formen $4n+3$ eller $4n+1$. Produkten av två tal på den senare formen, $4m+1$ och $4n+1$, är också på denna form: $4(4mn+m+n)+1$. Vad kan man då säga om faktoriseringar av tal på formen $4n+3$?

3. Låt F vara en största familj av k-delmängder till $\{1, 2, \ldots, n\}$ som är sådan att varje par av mängder i familjen har åtmistone ett element gemensamt. Visa att antalet mängder i F är åtminstone $\binom{n-1}{k-1}$.

   Tips! Vad gäller om alla mängderna i en familj innehåller elementet 1?

4. Låt $P(n)$ vara antalet heltalspartitioner av n. Visa att $P(n) \leq P(n+1)$.

5. En *artikulationspunkt* till en graf G är en nod x sådan att om den tas bort så går G sönder, dvs $\kappa(G) < \kappa(G - x)$. Visa att varje sammanhängande graf som har åtminstone två noder måste ha åtminstone två noder som inte är artikulationspunkter.

   Tips! Tänk på att varje sammanhängande graf har ett spännande träd. Hur många löv har ett träd med minst två noder? Kan ett löv vara artikulationspunkt?

6. Visa att om det finns två noder x och y i en sammanhängande graf så att det inte finns två noddisjunkta stigar mellan x och y så måste det finnas någon nod z så att alla stigar mellan x och y innehåller z.

   Tips! Kontraposition och steg-för-steg. Anta att man har hittat två stigar från x till y som är noddisjunkta fram till en gemensam nod z på avstånd $d \geq 1$ från y. Visa att det går att göra om den ena stigen så att den undviker z, och att stigarna därmed blir noddisjunkta fram till en gemensam nod på avstånd $d' < d$ från y.

7. Visa att om en graf är 2-sammanhängande så finns det två noddisjunkta stigar mellan varje par av noder som inte är grannar.

   Tips! Använd förra uppgiften.