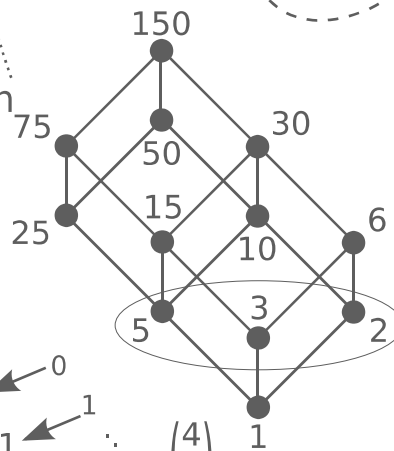
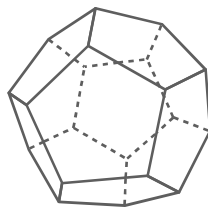
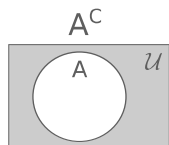
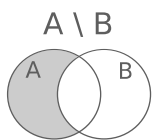
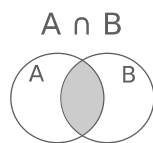
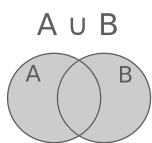
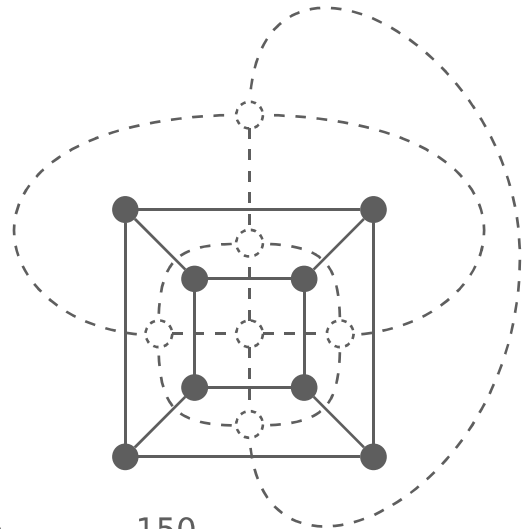
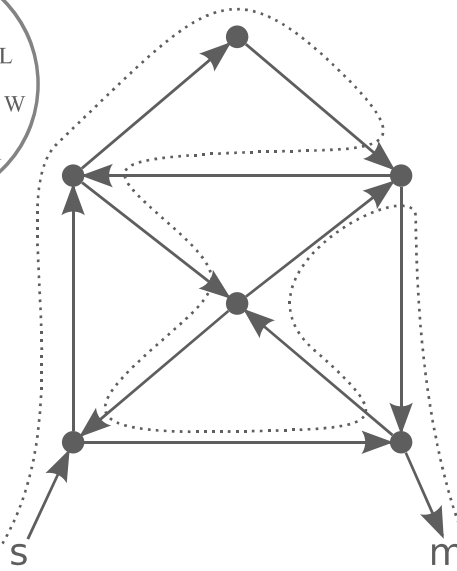
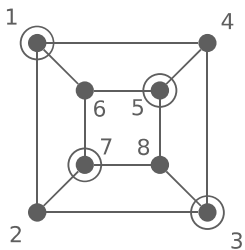
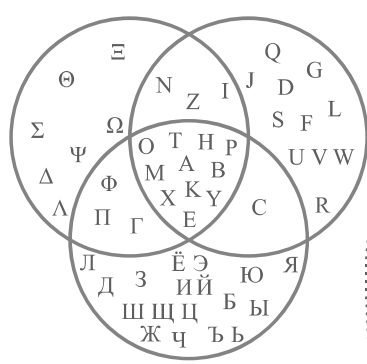
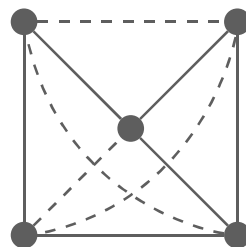
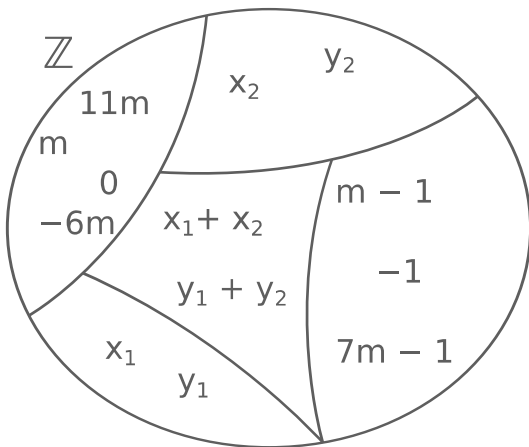
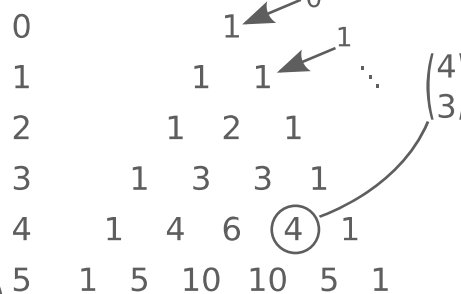


SF1610

Diskret matematik



Primtal
i 150



xy
 \bar{y}

xy	
\bar{x}	y
00	01
01	00
11	11
10	01

Modul 1

2011-(01)jan-15: dag 1, 1

SF1610 – Diskret matematik

Diskret = inkontinuerlig (inga derivator, integraler &c)

Kursintroduktion

Aritmetik och mängder (Heltalsräkning, primtal, med mera)
Kombinatorik (Räkna saker och möjligheter)
Algebra (Grupper, permutationer)
Tillämpad algebra

Kursens huvuddelar: (Motsvarar KS:arna)

Aritmetik och mängder

Exempel: Finn alla heltal, m och n , så att
 $31m + 15n = 102$

Exempel: Låt $a_0 = 0$, $a_1 = 1$, $a_2 = 1$, $a_3 = 2$,
 $a_4 = 3$, $a_5 = 5$, ... vad är $a_{1000000}$?

Kombinatorik

Exempel: n stycken brev stoppas i varsit slumpmässigt kuvert.
Hur stor sannolikhet är det att inget brev hamnar i
rätt kuvert?

Exempel: På hur många sätt kan 13 identiska vita kulor och 3
färgade olika kulor ordnas så att inga färgade kulor
ligger intill varandra?

Algebra, gruppteori


Exempel: Om p är ett primtal så är talet $(p - 1)! + 1$ delbart med p .

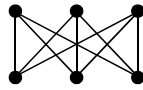
Exempel: Riffelblandning av en kortlek; hur många gånger behövs
den blandas för att återgå till ursprungliga tillståndet?

Tillämpad algebra

Koder, logiska kretsar.

Grafer och nätverk.

Exempel: Visa att minst  inte kan ritas utan två korsande linjer.



Idag om heltal, 3 kap. i först boken.

Division av heltal

 $\frac{37}{5}$? Inget heltal! $\begin{cases} \text{Rationella tal} \\ \text{Division med rest} \end{cases}$

37 delat med 5 get kvoten 7 med resten 2. Det vill säga $37 = 5 \cdot 7 + 2$.
 ↑
 Principala resten, $0 \leq r < 5$

Sats: Division med rest

Om heltalen p och $d \neq 0$ finns entydiga heltal q och r sådana att

$$p = \underset{\substack{\uparrow \\ \text{kvot}}}{q} \cdot d + \underset{\substack{\uparrow \\ \text{rest}}}{r}, \quad 0 \leq r < |d|$$

Bevis:

Låt $d > 0$ ($d < 0$ byter tecken på q)
 Betrakta alla heltal > 0 , av formen $p - ad$, $a \in \mathbb{Z}$

Finns minst ett sådant tal $(a = -|p| \Rightarrow p - ad = p + d|p| \geq 0)$

Låt r vara det minsta sådana talet.
($r = p - qd \geq 0$, $q = \text{lägsta}$)

Vi har då q och r så att $p = qd + r$, $0 \leq r < d$.

Kvar att visa: entydighet

$$\begin{aligned} \text{Om } p = qd + r = q'd + r, \quad 0 \leq r, r' < d \text{ då } (q - q')d = r' - r \\ q - q': \quad \text{heltal} \\ r' - r: \quad -d < r' - r < d \end{aligned}$$

Detta ger $q - q' = 0$, det vill säga $q = q'$, $r = r'$

Talbaser

Att skriva tal i basen t:

Låt x och t vara heltal ($x \geq 0, t \geq 2$)

(Det går att ha godtyckliga komplexa tal x , eller generellare, och reela, komplexa, eller generellare t med heltals komponent, och $|t| > 1$)

Dividera x med t:

$$\begin{array}{ll} x = q_0 t + r_0, & 0 \leq r_0 < t \\ q_0 = q_1 t + r_1, & 0 \leq r_1 < t \\ q_1 = q_2 t + r_2, & 0 \leq r_2 < t \\ q_2 = q_3 t + r_3, & 0 \leq r_3 < t \\ \vdots & \end{array}$$

$$q_{n-1} = q_n t + r_n, \quad q_n = 0, 0 \leq r_n < t \Rightarrow q_{n-1} = r_n$$

Detta ger:

$$\begin{aligned} \mathbf{x} &= \underbrace{(((\dots (\overbrace{(\mathbf{r}_n \cdot \mathbf{t} + \mathbf{r}_{n-1}) \mathbf{t} + \mathbf{r}_{n-2}) \mathbf{t} + \dots \mathbf{t} + \mathbf{r}_2) \mathbf{t} + \mathbf{r}_1) \mathbf{t} + \mathbf{r}_0)}_{\mathbf{q}_0} = \\ &= \mathbf{r}_n \mathbf{t}^n + \mathbf{r}_{n-1} \mathbf{t}^{n-1} + \dots + \mathbf{r}_1 \mathbf{t}^1 + \mathbf{r}_0 = \underbrace{(\mathbf{r}_n \mathbf{r}_{n-1} \mathbf{r}_{n-2} \dots \mathbf{r}_1 \mathbf{r}_0)}_{\mathbf{x} \text{ i basen } \mathbf{t}} \mathbf{t} \end{aligned}$$

Exempel

2011 i basen 11

$$\begin{array}{rcl}
 2011 & = & 182 \\
 \swarrow & & \\
 182 & = & 16 \\
 \swarrow & & \\
 16 & = & 1 \\
 \swarrow & & \\
 1 & = & \mathbf{0}
 \end{array}
 \quad
 \begin{array}{l}
 \cdot \underline{11} + 4 \\
 \cdot \underline{11} + 6 \\
 \cdot \underline{11} + 5 \\
 \cdot \underline{11} + 1
 \end{array}
 \left. \vphantom{\begin{array}{l} \cdot \underline{11} + 4 \\ \cdot \underline{11} + 6 \\ \cdot \underline{11} + 5 \\ \cdot \underline{11} + 1 \end{array}} \right\} \Rightarrow 2011_{10} = \underset{4}{1} \underset{3}{5} \underset{2}{6} \underset{1}{4}_{11}$$

Exempel

$$\underset{1}{2} \underset{2}{5} \underset{3}{1}_6 = 2 \cdot 6^2 + 5 \cdot 6^1 + 1 \cdot 6^0 = 2 \cdot 36 + 5 \cdot 6 + 1 = 72 + 30 + 1 = 103_{10}$$

Särskilt viktigt: Binära tal (2-bas)

$$\begin{array}{rcl} 2011 & = & 1005 \cdot 2 + 1 \\ 1005 & = & 502 \cdot 2 + 1 \\ 502 & = & 251 \cdot 2 + 0 \\ 251 & = & 125 \cdot 2 + 1 \\ 125 & = & 62 \cdot 2 + 1 \\ 62 & = & 31 \cdot 2 + 0 \\ 31 & = & 15 \cdot 2 + 1 \\ 15 & = & 7 \cdot 2 + 1 \\ 7 & = & 3 \cdot 2 + 1 \\ 3 & = & 1 \cdot 2 + 1 \\ 1 & = & 0 \cdot 2 + 1 \end{array} \left. \vphantom{\begin{array}{rcl} 2011 \\ 1005 \\ 502 \\ 251 \\ 125 \\ 62 \\ 31 \\ 15 \\ 7 \\ 3 \\ 1 \end{array}} \right\} 2011_{10} = 11111011011_2$$

Delbarhet, primtal &c

Om d och m är heltal:

$d|m$ läses som “ d delar m ”, “ d är en delare till m ”,
↑ “ m är en multipel av d ”...

En heltalsrelation

$d|m$ betyder att det finns ett heltal q sådant att $m = qd$,
det vill säga en kvot utan rest.

Exempel:

$$2|6, -8|24 \quad 14 \nmid 2, 5|0, 0 \nmid 7, -3|-18, 0|0.$$

Definition på primtal

Ett primtal är ett heltal $p > 1$ ($p \in \mathbb{P}$) som bara har delarna ± 1 och $\pm p$.

$$\mathbb{P} = \{2, 3, 5, 11, \dots, 113, \dots, 85218761, \dots\}$$

Det finns oändligt många primtal.

Största gemensamma delare, sgd (gcd)

Definition:

Om m, n är heltal är en sgd för m, n ett heltal d sådant att:

- 1) $d|m, d|n$ (är gemensam delare)
- 2) om $c|m, c|n \Rightarrow c | d$ (är störst)
- 3) $d \geq 0$ (är entydig) \leftarrow nästa föreläsning!

Exempel:

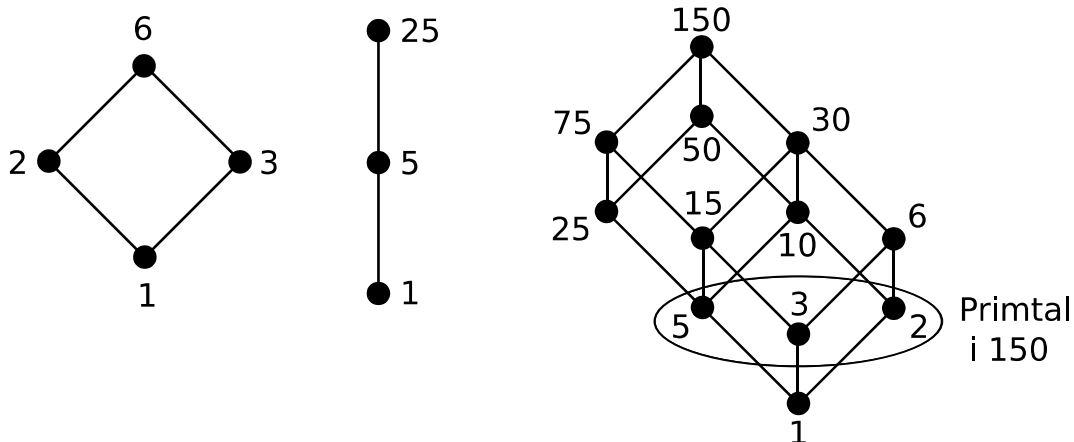
$$\begin{aligned} \text{sgd}(28; 49) &= 7 \\ \text{sgd}(11; 0) &= 11 & (11|0) \\ \text{sgd}(m; n) &= \text{sgd}(n; m) \\ \text{sgd}(m; 1) &= 1 \\ \text{sgd}(0; 0) &= 0 & (c|0) \\ \text{sgd}(\pm m; \pm n) &= \text{sgd}(m; n) \\ \text{sgd}(m; n) &= \text{sgd}(m + kn; n) \text{ ty } c|m, c|n \Leftrightarrow c|(m + kn), c|n \end{aligned}$$

Speciellt:

$$\text{sgd}(m; n) = \text{sgd}(n; m - qn)$$

Delargrafen för ett heltal $g > 0$:

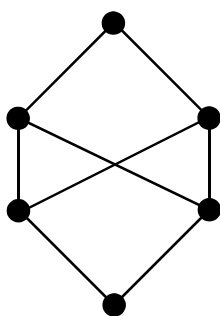
Punkter svarar mot all talets delare,
uppåtriktade streck från "direkta delare".



En gemensam delare till m, n i en delargraf:

Ett tal ligger under båda

Att det finns en entydig största gemensamma delare ger ett villkor på hur delargrafen kan se ut.



Finns ingen sådan delargraf.
Ty 0 saknar sgd.

2011-(01)jan-17: dag 2, 2

Aritmetikens fundamentalsats

Alla positiva heltal (större än 1) kan faktoriseras till en unik mängd av (icke-unika) primtal.

Diofantiska ekvationer

Endast heltalslösningar.

Euklides' algoritm

Ger största gemensamma delaren.

Lemma:

Om $d|a$ (d delar a) och $d|b$ så $d|(na + mb)$ för alla heltal n och m .

Bevis:

$d|a$ innebär att $a = kd$
 $d|b$ innebär att $b = k'd$

Då gäller:

$$na + mb = nkd + mk'd = d(nk + mk') = dp, p \in \mathbb{Z}$$

Exempel:

Bestäm $\text{sgd}(217; 314)$

↑
största gemensamma delare (en. gcd; greatest common divider)

Lösning:

Med hjälp av Euklides' algoritm

$$314 = 1 \cdot 217 + 97$$

$$217 = 2 \cdot 97 + 23$$

$$97 = 4 \cdot 23 + 5$$

$$23 = 5 \cdot 5 - 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$\text{eller } 23 = 4 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$\text{Alltså } 1 = \text{sgd}(314; 217)$$

Om $d|314$ och 217
så $d|(1 \cdot 314 - 1 \cdot 217)$,
det vill säga $d|97$.

$$d|217 \wedge d|97 \Leftrightarrow \\ \Leftrightarrow d|(217 - 2 \cdot 97) \Leftrightarrow d|23$$

$$d|23 \wedge d|5 \Leftrightarrow d|(5 \cdot 5 - 23)$$

Exempel:

Sök $\text{sgd}(332; 512)$

Lösning:

$$512 = 2 \cdot 332 - 152$$

$$332 = 2 \cdot 152 + 28$$

$$152 = 5 \cdot 28 + 12$$

$$28 = 2 \cdot 12 + 4$$

$$12 = 3 \cdot 4 + 0$$

$$4|4 \wedge 4|12 \Rightarrow 4|28$$

$$4|12 \wedge 4|28 \Rightarrow 4|28$$

och så vidare

$$4|512 \wedge 4|332$$

Den sista icke-försvinnande: 4

Resten är sgd så:

$$\text{Svar: } \text{sgd}(332; 512) = 4$$

En diofantisk ekvation:

Exempel: Bestäm hela tal, x och y , sådana att $x \cdot 512 + y \cdot 332 = 4$

Lösning: Använder Euklides' algoritm; se ovan

Vi får ur detta att

$$\begin{aligned} 4 &= 28 - 2 \cdot 12 = \\ &= 28 - 2(152 - 5 \cdot 28) = \\ &= 11 \cdot 28 - 2 \cdot 152 = \\ &= 11 \cdot (332 - 2 \cdot 152) - 2 \cdot 152 = \\ &= 11 \cdot 332 - 22 \cdot 152 - 2 \cdot 152 = \\ &= -24 \cdot 152 + 11 \cdot 332 = \\ &= -24(2 \cdot 332 - 512) + 11 \cdot 332 = \\ &= -48 \cdot 332 + 24 \cdot 512 + 11 \cdot 332 = \\ &= \underbrace{-37 \cdot 332}_y + \underbrace{24 \cdot 512}_x \end{aligned}$$

Svar: $x = 24$, $y = -37$

Sats:

Antag att $D = \text{sgd}(a; b)$; då finns alltid tal, x och y , sådana att $D = xa + yb$.

Exempel:

Bestäm en lösning till den diofantiska ekvationen

$$63x + 97y = 1$$

Lösning:

Euklides' algoritm

$$97 = 1 \cdot 63 + 34$$

$$63 = 2 \cdot 34 - 5$$

$$24 = 7 \cdot 5 - 1$$

Vi finner av algoritmen

$$1 = 7 \cdot 5 - 34 = 7 \cdot (2 \cdot 34 - 63) - 34 =$$

$$= 13 \cdot 34 - 7 \cdot 63 = 13(97 - 63) - 7 \cdot 63 =$$

$$= 13 \cdot 97 - 20 \cdot 63$$

Svar: $y = 13$, $x = -20$

Lemma:

Antag att p är ett primtal ($p \in \mathbb{P}$).

Då gäller att $p|a \cdot b \Rightarrow p|a \vee p|b$

↑
och/eller

↑
"eller" betyder och/eller, alltså inklusivt eller
precis som i vanligt språk. Exklusivt eller,
kan skrivas till exempel \oplus eller $\underline{\vee}$ och kallas
XOR (vanligast), EOR, "exklusivt eller", eller
som i vanligt språk: "antingen ... eller ...".

$p \nmid a \Rightarrow \text{sgd}(p; a) = 1$ ty enda kandidaterna till sgd är 1
ty $p \nmid a$ och $a \nmid p$ ty $p \in \mathbb{P}$.

Det finns n och m sådana att $1 = np + ma$.

Multiplikera med b : $b = npb + mab$

$p|ab, p|p \Rightarrow p|(npb + mab)$ så $p|b$ eftersom $p|ab$.

Bevissats:

Steg 1: Visa att det finns minst en primtalsfaktorisering.

Fall 1: n är ett primtal. Klar!

Fall 2: n är ej ett primtal

$$n = a \cdot b, a, b > 1$$

Fortsätt med a och b och försök faktorisera dess tal.
Och så vidare.

Steg 2: Visa att faktoriseringen är unik.

Antag att faktoriseringen inte är unik, det vill säga

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_e$$

Ej nödvändigtvis olika primtal.

Då gäller $p_1 | n$ så: $p_1 | q_1(q_2 \cdot \dots \cdot q_e)$

Fall 1: $p_1 | q_1 \Rightarrow p_1 = q_1$, ty primtal har (per definition) inga andra delare jämte sig själva.

Fall 2: $p_1 | p_1 \Rightarrow p_1 | (q_2 \cdot \dots \cdot q_e) \Rightarrow p_1 | q_2(q_3 \cdot \dots \cdot q_e)$ och så vidare.

Tillslut hittar vi ett q_i sådant att $p_1 | q_i$ och $p_1 = q_i$.

Börja från början med $n' = \frac{n}{p_1} = \frac{n}{q_i}$.

$$n' = p_2 p_3 \dots p_k = q_2 q_3 \dots q_e \quad (\text{ifall } p_1 = q_1 \text{ (} i = 1 \text{)})$$

Exempel:

Bestäm samtliga lösningar till den diofantiska ekvationen $63x + 97y = 1$.

Lösning:

Vi har från tidigare $x = -20, y = 13$.

Antag att x', y' är en annan lösning:

$$\begin{array}{rcl} 13 \cdot 97 & -20 \cdot 63 = 1 & \\ - y' \cdot 97 & + x' \cdot 63 = 1 & \\ \hline (13 - y') \cdot 97 & + (-20 - x') \cdot 63 = 0 & \end{array}$$

Observera att övre raden subtraheras med undre raden ($y' \cdot 97 + x' \cdot 63$). $-$:et är alltså en operation mellan raderna, i båda kolonnerna.

\Downarrow

$$(13 - y') \cdot 97 = (20 + x') \cdot 63$$

Relativt prima

Vi vet att $\text{sgd}(63; 97) = 1$ så $63 | (13 - y')$.

Det vill säga

$$\begin{aligned} 13 - y' &= k \cdot 63 \\ y' &= 13 - k \cdot 63 \end{aligned}$$

Vi får att

$$\begin{aligned} k \cdot 63 \cdot 97 &= (20 + x') \cdot 63 \\ k \cdot 97 &= 20 + x' \\ x' &= -20 + k \cdot 97 \end{aligned}$$

Svar:

$$\begin{aligned} x' &= -20 + k \cdot 97 \\ y' &= 13 - k \cdot 63 \\ k &= 0, \pm 1, \pm 2, \dots \quad (k \in \mathbb{Z}) \end{aligned}$$

Om x', y' är en lösning så är

$$\begin{aligned} x' &= -20 + k \cdot 97 \\ y' &= 13 - k \cdot 63 \end{aligned}$$

för något $k \in \mathbb{Z}$.

Vi måste verifiera att vi får en lösning för olika k , vilket är lätt:

$$\begin{aligned} 63(-20 + k \cdot 97) + 97(13 - k \cdot 63) &= \\ = -20 \cdot 63 + k \cdot 63 \cdot 97 + 13 \cdot 97 - k \cdot 63 \cdot 97 &= \\ = -20 \cdot 63 + 13 \cdot 97 &= \mathbf{1} \end{aligned}$$

Exempel:

Lös ekvationen $36x + 56y = 2$

Lösning:

$$36x + 56y = 2$$

$$18x + 28y = 1$$

Saknar lösning ty $\text{sgd}(18; 28) \nmid 1$

Exempel:

Bestäm en lösning till $63x + 97y = 113$

Lösning:

$$\text{Vi vet att } -20 \cdot 63 + 13 \cdot 97 = 1$$

$$113 \cdot (-20) \cdot 63 + 113 \cdot 13 \cdot 97 = 113$$

$$x = 113 \cdot (-20) = -2260$$

$$y = 113 \cdot 13 = 1599$$

2011-(01)jan-24: dag 3, 3

Övning idag

1) Beräkna $a + b$, $c \cdot d$ med $a = 218$, $b = 137$, $c = 89$, $d = 43$ (bas 10)

- a) I bas 10
- b) I bas 2
- c) I bas 7

a)	$\begin{array}{r} \underline{1} \\ 218 \\ +137 \\ \hline 355 \end{array}$	$\begin{array}{r} 89 \\ \cdot 43 \\ \hline 167 \\ +356 \\ \hline 3827 \end{array}$	verifiera första	$\begin{array}{r} \underline{10} \\ 355 \\ -137 \\ \hline 218 \end{array}$
----	---	--	---------------------	--

b) Uttryck a , b , c , d i bas 2:

$218 = 2 \cdot 109 + 0$	så:	$a = 11011010_2$
$109 = 2 \cdot 54 + 1$	på samma sätt:	$b = 10001001_2$
$54 = 2 \cdot 27 + 0$		$c = 1011001_2$
$27 = 2 \cdot 13 + 1$		$d = 101011_2$
$13 = 2 \cdot 6 + 1$		
$6 = 2 \cdot 3 + 0$		
$3 = 2 \cdot 1 + 1$		
$1 = 2 \cdot 0 + 1$		

a + b)

$$\begin{array}{r} 11011010 \\ +10001001 \\ \hline 101100011 \end{array}$$

Verifiera:

$$\begin{array}{r} 2 \quad 22 \\ 101100011 \\ -10001001 \\ \hline 11011010 \end{array}$$

c · d) Gör själv!

c) Bas 7

$$\begin{aligned} 218 &= 7 \cdot 31 + 1 \Rightarrow a = 431_7 \\ 31 &= 7 \cdot 4 + 3 \\ 4 &= 7 \cdot 0 + 4 \end{aligned}$$

På samma sätt: $b = 254_7$
 $c = 155_7$
 $d = 61_7$

Även förekommande att skiva 431_{sju} , $431_{\text{"sju"}}$ (vanliga i grundskolan) eller speciellt i denna kurs $(431)_7$ (vilket dock är tvetydligt, vilket vi kommer se senare).

$$\begin{array}{r} 155 \\ \cdot 61 \\ \hline 155 \\ +1362 \\ \hline 14105 \end{array} \quad 6 \cdot 5 = 42_7$$

2) $n = 10'1100'1111'0101_2 = 2CF5_{16} = \{10'110'011'110'101_2\} = 26365_8$

16-tal 8-tal

$$m = 364401_8 = 11'110'100'100'000'001_2 = 1E901_{16}$$

3) $\text{sgd}(2373; 1638) ?$ största gemensama delaren

$$\text{sgd}(m; n) = \text{sgd}(n; m - kn)$$


$$\begin{aligned} 2373 &= 1 \cdot 1638 + 735 \\ 1638 &= 2 \cdot 735 + 168 \\ 735 &= 4 \cdot 168 + 63 \\ 168 &= 2 \cdot 63 + 42 \\ 63 &= 1 \cdot 42 + 21 \\ 42 &= 2 \cdot 21 + 0 \end{aligned}$$

Så största gemensama delaren är 21
 $\text{sgd}(2373; 1638) = 21$

$$\text{mgm}(2373; 1638) ?$$

mgm = minsta gemensamma multipel

$$\begin{aligned} \text{sgd}(m; n) \cdot \text{mgm}(m; n) &= m \cdot n = \\ &= \frac{2373 \cdot 1638}{21} = \dots = 113 \cdot 1638 = 185094 \end{aligned}$$




4) k heltal

$$\begin{aligned} \text{sgd}(3k + 2; 5k + 3) &= \leftarrow ((5k + 3) - (3k + 2) = 2k + 1) \\ &= \text{sgd}(3k + 2; 2k + 1) = \leftarrow ((3k + 2) - (2k + 1) = k + 1) \\ &= \text{sgd}(k + 1; 2k + 1) = \\ &= \text{sgd}(k + 1; k) = \text{sgd}(1; k) = 1 \end{aligned}$$

5) Emma har 75 kr i 1-, 5- & 10-kr-mynt.
Totalt har hon 16 mynt.
Hur många har hon av varje sort?

Antag att gon har x stycken 1 kr, y stycken 5 kr, z stycken 10 kr.

$$\begin{cases} x + 5y + 10z = 75 \\ x + y + z = 16 \\ x, y, z \text{ heltal} \geq 0 \end{cases}$$

Ett diofantiskt ekvationssystem.

 (Vi söker heltalslösningar)

$$x + 5y + 10z - x - y - z = 75 - 16 \quad (x \text{ elimineras})$$

$$4y + 9z = 59$$

$$\begin{aligned} \text{sgd}(4, 9) &= 1 \\ \text{sgd}(m; n) &= ma + nb \end{aligned}$$

Så

$$4 \cdot (-118) + 9 \cdot 59 = 59$$

Så en lösning till till ekvationen

$$\begin{cases} y_0 = -118 \\ z_0 = 59 \end{cases}$$

Om y, z är en lösning:

$$4(y - y_0) + 9(z - z_0) = 0$$

$$4(y - y_0) = -9(z - z_0)$$

4 & 9 är relativt prima

$$\begin{aligned} \text{så} \quad z &= z_0 - 4k \\ y &= y_0 - 9k \end{aligned}$$

Vilket k ?

$$y, z \geq 0, \quad 59 + 4k \geq 0 \quad \text{ger}$$

$$k \geq -\frac{59}{4} = -14\frac{3}{4}$$

$$-118 - 9 \leq 0 \quad \text{ger} \quad k \leq -\frac{118}{9} = -13\frac{1}{9}$$

$$\text{Det vill säga} \quad k = -14$$

Så enda lösningen till ekvationen med $y, z > 0$:

$$y = -118 - 9(-14) = 8$$

$$z = 59 + 4(-14) = 3$$

$$\text{Motsvarande} \quad x = 16 - 3 - 8 = 5$$

Så Emma har
5 stycken 1-kr,
8 stycken 5-kr och
3 stycken 10-kr.

- 6) Visa att om $am + bn = 1$ så $\text{sgd}(m; n) = 1$ (a, b, m, n heltal)
 $d|m, d|n \Rightarrow d|am + bn = 1$ så $d = \pm 1$ så $\text{sgd}(m; n) = 1$

- 8) Primtalsfaktorisera talen 111, 467, 314000 och 10300_6 (det talet som i bas 6 skrivs 10300).

$$111 = 3 \cdot 37$$

467 Man testar primtal till man kommer upp till ett tal vars kvadrart är större än talet.

$$\begin{aligned} 314000 &= 314 \cdot 1000 = 2 \cdot 157 \cdot 1000 = & \{157 \text{ är ett primtal}\} \\ &= 2 \cdot 157 \cdot 10^3 = 2 \cdot 157 \cdot 2^3 \cdot 5^3 = \\ &= 2^4 \cdot 5^3 \cdot 157 \end{aligned}$$

$$103000_6 = 103_6 \cdot 6^2 = 39 \cdot 2^2 \cdot 3^2 = 2^2 \cdot 3^3 \cdot 13$$

- 10) $10|n^2 \Leftrightarrow 2, 5|n^2 \Leftrightarrow 2, 5|n \Leftrightarrow 10|n$

Svar: Ja

$$9|n^2 \Leftrightarrow 3|n \quad \text{Motexempel:} \quad n = 3$$

$$\text{Svar: Nej} \quad 9|3^2 = 9, \quad 9 \nmid 3$$

- 11) a, b, c bland 0, 1, ..., 9

$(abc \ abc)_{10}$ delbart med 3 olika primtal.

$$(abc \ abc)_{10} = (abc)_{10} \cdot 1001$$

$$1001 = 7 \cdot 11 \cdot 13$$

2011-(01)jan-25: dag 4, 4

Sist:

Sats: Om m, n är heltal (båda $\neq 0$) existera $\text{sgd}(m; n)$ entydligt och är $am + bn$, några heltal a, b .

Euklides' algoritm:

$$(\text{sgd}(m; n) = \text{sgd}(n; m - qn) \text{ upprepat } \text{sgd}(d; 0) = d)$$

Tag $m \geq n \geq 0$

$$\begin{array}{ll} m = q_1 n + r_1 & 0 \leq r_1 < n \\ n = q_2 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = q_3 r_2 + r_3 & 0 \leq r_3 < r_2 \\ r_2 = q_4 r_3 + r_4 & 0 \leq r_4 < r_3 \\ \vdots & \vdots \end{array}$$

$$\begin{array}{ll} r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} = q_k r_{k-1} + \mathbf{0} \end{array} \quad (\text{slutar allt med } \mathbf{0})$$

$$r_{k-1} = \text{sgd}(m; n)$$

$$r_{k-1} = r_{k-3} - q_{k-1} r_{k-2} = \dots$$

Följdsats: Om $d|mn$ och $\text{sgd}(d; m) = 1$ så $d|n$
 \uparrow
 d, m relativt prima

För alla heltal k, m, n :

$$m|m, k|n, m|n \Rightarrow k|m$$

Definition: Om m, n är heltal så är en minsta gemensamma multipel, mgm (en. lcm) för m, n ett heltal g sådant att

- i) $m, n | g$
- ii) $m, n | n \Rightarrow g|h$
- iii) $g \geq 0$

Sats: Om m, n är heltal så existerar $\text{mgm}(m; n)$ entydigt och uppfyller
 $\text{mgm}(m; n) \cdot \text{sgd}(m; n) = mn$

$$(\text{mgm}(0; 0) = 0)$$

Sats: Den linjära diofantiska ekvationen (heltalslösningar sökes)

$$mx + ny = c$$

har lösningar om $\text{sgd}(m; n) \mid c$.

Om $\text{sgd}(m; n) = am + bn$, a, b heltal ges alla lösningar av

$$\begin{cases} x = a\frac{c}{d} + q\frac{n}{d} \\ y = b\frac{c}{d} - q\frac{m}{d} \end{cases} \quad q \text{ heltal}$$

Definition: Ett primtal är ett heltal $p > 1$ som bara har delarna ± 1 och $\pm p$.

Exempel: 2, 3, 17, 101, 123449

Aritmetikens fundamentalsats:

Varje heltal ≥ 1 kan på ett entydigt (bortsätt från ordningen) sätt skrivas som en produkt av primtal

$$\text{sgd}(p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}; p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}) = p_1^{\min(s_1; t_1)} p_2^{\min(s_2; t_2)} \dots p_k^{\min(s_k; t_k)}$$

Likadant för mgm , fast \max istället för \min .

Så $\text{sgd}(m; n) \cdot \text{mgm}(m; n) = mn$.

Euklides: Det finns oändligt många primtal.

$$\left(\text{Det gäller att } \sum_{p \in \mathbb{P}} \frac{1}{p} = \infty \right)$$

Idag:

Modulär aritmetik, \mathbb{Z}_m

Räkna med rester (mod m)

+ och \times -tabeller i \mathbb{Z}_m

Inverterbara (invertibla) element i \mathbb{Z}_m

Linjära ekvationer

$$ax + b \quad \text{i } \mathbb{Z}_m$$

Lite mängdlära

$$\{x \mid \dots\dots\dots\}$$

$$a \in A, \quad A \subseteq B$$

$$|A|, \quad A \cup B, \quad A \cap B, \quad A \setminus B, \quad A^c, \quad \mathcal{P}(A)$$

Räkneregler för $\cap, \cup, ^c, \emptyset, \mathcal{U}$

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

Produktmängden $A \times B$

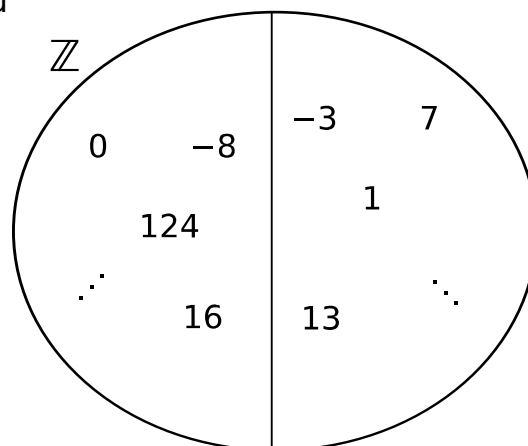
Idag, först, om modulär aritmetik

Minns "räkneregler" för jämna (j) och udda (u) tal

$$\begin{array}{llll} j + j = j, & j + u = u, & u + j = u, & u + u = j \\ j \cdot j = j, & j \cdot u = j, & u \cdot j = j, & u \cdot u = u \end{array}$$

+	j	u
j	j	u
u	u	j

\cdot	j	u
j	j	j
u	j	u



Allmänt med $m \geq 2$ heltal.

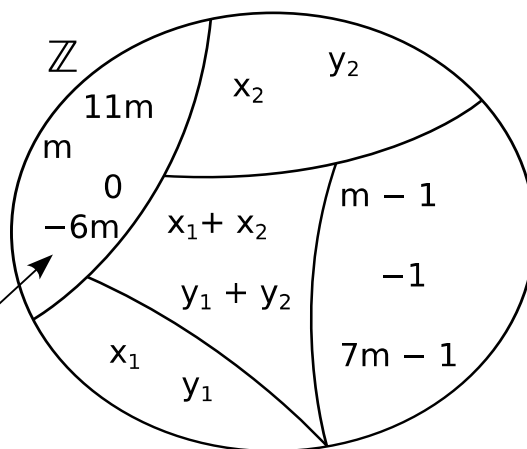
Att räkna modulo m

$$x \equiv y \pmod{m} \stackrel{\text{def}}{\Leftrightarrow} m \mid (x - y)$$

↑
eller $x \equiv_m y$

“kongruenta modulo m”

Resten 0 vid ÷ med m



x och y ger samma rest vid division med m.

Då: $x_1 \equiv_m y_1, x_2 \equiv_m y_2 \Rightarrow x_1 + x_2 \equiv_m y_1 + y_2$

$$x_1 \cdot x_2 \equiv_m y_1 \cdot y_2$$

$$qm + r_1 \equiv_m q'm + r_1$$

Man skriver ofta = (istället för \equiv) och säger att man räknar i $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$

Tabeller i \mathbb{Z}_m

$$\mathbb{Z}_3$$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$\mathbb{Z}_4$$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Exempel:

Vad blir (principala) resten då 67^{380} divideras med 31?

Det vill säga; vad är $67^{380} \bmod 31$?

$$67^{380} \equiv_{31} (67 \bmod 31)^{380} = 5^{380} = 5^{3 \cdot 126 + 2} = 125^{126} \cdot 5^2 \equiv$$

$$\{125 = 4 \cdot 31 + 1 \equiv_{31} 1\} \equiv_{31} 1^{126} \cdot 25 = 1 \cdot 25 = \underline{25}$$

$$5^{380} = \underbrace{(((\dots((1 \cdot 5)^2 \cdot 1)^2 \cdot 5)^2 \dots 5)^2 \cdot 1)^2 \cdot 1}_{\times 8} \underbrace{\dots}_{\times 5}$$

Allt räknat modulo 31

ty $380 = 101111100_2$

De flesta räkneregler i \mathbb{Z}_m är samma som i \mathbb{Z} ,
men man kan ha $x \cdot y = 0$ i \mathbb{Z}_m fast $x, y \neq 0$ i \mathbb{Z}_m .
Till exempel $3 \cdot 4 = 0$ i \mathbb{Z}_6 .

Definition: r i \mathbb{Z}_m är invertibel om det finns x i \mathbb{Z}_m så att $rx = 1$ i \mathbb{Z}_m , $x = r^{-1}$.

Exempel: I \mathbb{Z}_4 är 1 och 3 invertibla, men inte 0 och 2.

$$1^{-1} = 1 \quad 3^{-1} = 3 \quad \text{ty} \quad 1 \cdot 1 = 1 \quad \text{och} \quad 3 \cdot 3 = 9 = 1$$

$$3x = 2 \quad \text{i } \mathbb{Z}_4$$

$$\text{ger} \quad 3 \cdot 3x = 3 \cdot 2 = 2 \quad \text{i } \mathbb{Z}_4$$

Sats: $r \in \mathbb{Z}_m$ är invertabel om $\text{sgd}(r; m) = 1$.

ty: r är invertabel i $\mathbb{Z}_m \Leftrightarrow rx \equiv_m 1$,
något $x \in \mathbb{Z} \Leftrightarrow rx - 1 = km$,
några $x, k \in \mathbb{Z} \Leftrightarrow rx - km = 1$,
några $x, k \Leftrightarrow \text{sgd}(r; m) = 1$.

Så i \mathbb{Z}_p , $p \in \mathbb{P}$, är alla utom 0 invertibla.

Exempel: Vad är 11^{-1} i \mathbb{Z}_{32} ?

Vi ser att $11 \cdot 3 = 33 \equiv_{32} 1$, så $11^{-1} = 3$. $\left(" \frac{1}{11} = 3 " \right)$

$11x = 7$ i \mathbb{Z}_{32} har lösningen $x = 3 \cdot 7 = 21$ i \mathbb{Z}_{32} .

$11x = 26$ i \mathbb{Z}_{32} har lösningen $x = 3 \cdot 26 = 14$ i \mathbb{Z}_{32} .

Exempel: Bestäm 11^{-1} i \mathbb{Z}_{47}

$\text{sgd}(11; 47) = 1$, så 11^{-1} existerar. Vad är den?

Euklides' algoritm:

$$\begin{aligned} 47 &= 4 \cdot 11 + 3 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 2 = 3 - (11 - 3 \cdot 3) = -11 + 4 \cdot 3 = \\ &= -11 + 4(47 - 4 \cdot 11) = 4 \cdot 47 - 17 \cdot 11 = \\ &= 4 \cdot 47 - 11 \cdot 47 + 47 \cdot 11 - 17 \cdot 11 = \\ &= -7 \cdot 47 + 30 \cdot 11 \end{aligned}$$

så $11 \cdot 30 = 1$ i \mathbb{Z}_{47} .

$11^{-1} = 30$ i \mathbb{Z}_{47} .

(Alternativt: $11^{-1} = -17 = 30$ i \mathbb{Z}_{47})

Den linjära ekvationen

$$ax = b \text{ i } \mathbb{Z}_m \quad (ax \equiv b \pmod{m})$$

Ekvationen är ekvivalent med den diofantiska ekvationen

$$ax - km = b$$

så lösningar finns om $\text{sgd}(a; m) | b$.

Exempel:

$$\text{Lös } 5x \equiv 4 \pmod{11}$$

Euklides':

$$\begin{aligned} 11 &= 2 \cdot 5 + 1 \\ 1 &= 11 - 2 \cdot 5 \end{aligned}$$

$$\text{Så } 4 = 4 \cdot 11 - 5 \cdot 8 = 4 \cdot 11 - 5 \cdot 11 + 11 \cdot 5 - 8 \cdot 5 = -11 + 3 \cdot 5.$$

$$\text{Och allmän lösning: } x = 3 + q \cdot 11, q \in \mathbb{Z}$$

$$\text{Entydig lösning i } \mathbb{Z}_{11}, \text{ ty } \text{sgd}(5; 11) = 1$$

Alternativt:

$$5x \equiv_{11} 4 \Leftrightarrow 2 \cdot 5x \equiv_{11} 2 \cdot 4 \Leftrightarrow -x \equiv_{11} 8 \Leftrightarrow x \equiv_{11} 3$$

\swarrow
 $\Leftarrow: \text{sgd}(2; 11) = 1$

Exempel:

$$\text{Lös } 5x \equiv_{15} 7$$

$$\text{Inga lösningar, ty } \text{sgd}(5; 15) = 5 \nmid 7.$$

$$(15 \nmid 5x - 7, \text{ ty } 5 \nmid 5x - 7)$$

Exempel:

$$\text{Lös } 5x \equiv_{15} 10$$

$$\text{Lösbar ty } \text{sgd}(5; 15) = 5 \mid 10$$

$$5x - k \cdot 15 = 10 \Leftrightarrow x - 3k = 2 \Leftrightarrow x = 3k + 2, \quad k \in \mathbb{Z}$$

Allmänt:

$$d = \text{sgd}(a; m)$$

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\text{mod } \frac{m}{d} \right)$$

Exempel:

$$\text{Lös } \begin{cases} 2x + 3y = 2 \\ 4x + 2y = 1 \end{cases} \text{ i } \mathbb{Z}_5 \quad (5 \text{ i } \mathbb{Z}_5 \text{ är primtal så alla utom 0 är invertibla.})$$

Som vanligt:

$$\left(\begin{array}{cc|c} 2 & 3 & 2 \\ 4 & 2 & 1 \end{array} \right) \xrightarrow{r_2 - 2 \cdot r_1} \left(\begin{array}{cc|c} 2 & 3 & 2 \\ 0 & 1 & 2 \end{array} \right) \xrightarrow{r_1 - 3 \cdot r_2} \left(\begin{array}{cc|c} 2 & 0 & 1 \\ 0 & 1 & 2 \end{array} \right) \xrightarrow{3 \cdot r_1} \left(\begin{array}{cc|c} 1 & 0 & 3 \\ 0 & 1 & 2 \end{array} \right)$$

$$\text{så } \begin{cases} x = 3 \\ y = 2 \end{cases} \text{ i } \mathbb{Z}_5.$$

Betyder att rad 2 subraheras med $2 \cdot$ rad 1.

Notera: Om $\text{sgd}(m; n) = 1$

$$a \equiv b \pmod{mn} \Leftrightarrow \begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$$

$$\text{ty: } \Rightarrow: \quad \underbrace{mn \mid a - b}_{= hmn} \Rightarrow m, n \mid \underbrace{a - b}_{(hn)m - (hm)n}$$

$$\begin{aligned} \Leftarrow: \quad m, n \mid a - b &\Rightarrow a - b = km \text{ och} \\ n \mid km &\Rightarrow a - b = km \text{ och} \\ n \mid k &= qn, \text{ det vill säga} \\ a - b &= qmn. \end{aligned}$$

Lite mängdlära (matematikens språk) (2 kap.)

Vi kan tänka på mängder som "påsar" med (pekare till) "saker" (element).

Exempel: $A = \{\text{Kalle, Olla, Lisa}\}$ (Kalle, Olla, Lisa är mängdes element.)

$$B = \{\sqrt{2}, c, -7, i\}$$

$$C = \{n \mid n \text{ är ett heltal och } n^2 \equiv_4 1\} = \{ \text{udda heltal} \} \quad (n \equiv_2 1)$$

$$\{\cdot \mid \dots\} \quad \text{"mängdbyggaren"}$$

$$\emptyset = \{x \mid x \neq x\} = \{\} \quad \text{Den tomma mängden}$$

Två mängder är lika om de innehåller samma element.

$\{\emptyset\}$ är inte \emptyset , utan en mängd som innehåller \emptyset .

Standardbeteckningar:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\} \quad \text{heltalen}$$

$$\mathbb{N} = \{\mathbf{0}, 1, 2, \dots\} \quad \text{de naturliga talen}$$

$$\mathbb{Z}_+ = \{\mathbf{1}, 2, \dots\} \quad (\mathbb{Z}^+ \text{ används också})$$

$$\mathbb{Q} = \{n \div m \mid m, n \in \mathbb{Z}, n \neq 0\} \quad \text{rationella talen}$$

$$\mathbb{R} \quad \text{reella talen}$$

$$\mathbb{C} \quad \text{complexa talen}$$

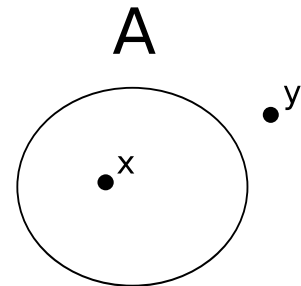
$$\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}$$

2011-(02)feb-02: dag 5, 5

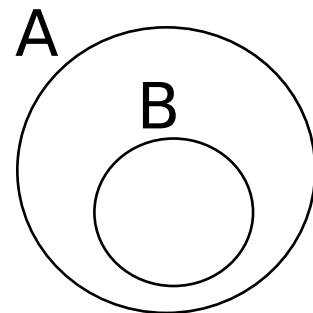
Flera beteckningar för mängdbegrepp

$x \in A$ x är ett element i A .

$y \notin A$ y är inte ett element i A .

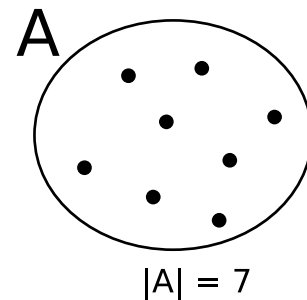


$A \subseteq B$ A är en delmängd till B ; A kan vara B .
 $x \in A \Rightarrow x \in B$ ($x \in B \ \forall \ x \in A$)
 $\exists x \in B : x \in A$



$A \subset B$ A är en delmängd (äka delmängd) till B ;
 A kan inte vara B .
 $\exists x \in B : x \in A, \exists x \in B : x \notin A$

$|A|$ Antalet element i A
 A :s kardinalitet (ordning)



$|\emptyset| = 0$ $|\{\emptyset\}| = 1$

Operationer på mängder

$A \cup B$ Unionen av A och B
 $\{x \mid x \in A \vee x \in B\}$

$A \cap B$ Snittet (skärningen) av A och B
 $\{x \mid x \in A \wedge x \in B\}$

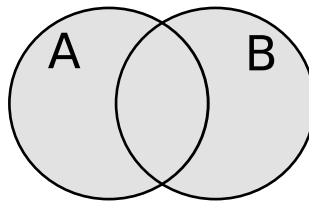
$A \setminus B$ Differansmängden (differansen mellan A och B)
 $\{x \mid x \in A \wedge x \notin B\}$

A^c Komplementmängden
(komplementet till A)

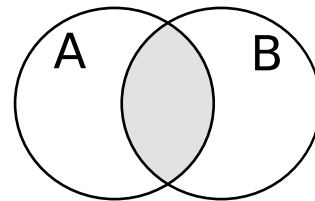
$$\{x \mid x \notin A\}$$

Skrivs även
 $\complement A$ eller CA (den innan
i sans-teckensnitt istället
för sans-serif)

$A \cup B$



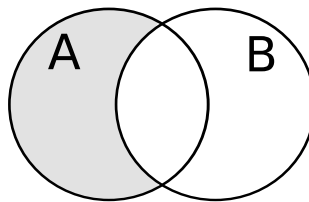
$A \cap B$



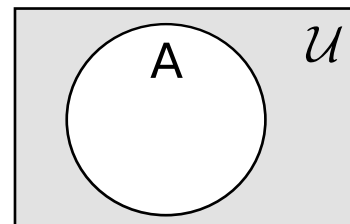
$\mathcal{P}(A)$ Potensmängden till A
Mängden av alla A:s
delmängder.

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

$A \setminus B$



A^c



Exempel:

$$\mathcal{P}(\{\emptyset, 1, \pi\}) = \{\emptyset, \{\emptyset\}, \{1\}, \{\pi\}, \{\emptyset, 1\}, \{\emptyset, \pi\}, \{1, \pi\}, \{\emptyset, 1, \pi\}\}$$

Kan även skrivas:

$$\mathcal{P}(A)$$

$$\wp(A)$$

$$2^A$$

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

$$A \subseteq B \Rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$$

$$C \subseteq A, A \subseteq B \Rightarrow C \subseteq B$$

Associativa lagen: $(A \cup B) \cup C = A \cup (B \cup C)$
 $(A \cap B) \cap C = A \cap (B \cap C)$

Kommutativa lagen: $A \cup B = B \cup A$
 $A \cap B = B \cap A$

Distributiva lagen: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgans lag: $(A \cup B)^c = A^c \cap B^c$
 $(A \cap B)^c = A^c \cup B^c$

Identitetslagar: $A \cup A = A$
 $A \cap A = A$
 $A \cap \mathcal{U} = A$
 $A \cup \emptyset = A$

Absorptionslagen: $A \cup (A \cap B) = A \cap (A \cup B) = A$

Dubbelt komplement: $(A^c)^c = A$

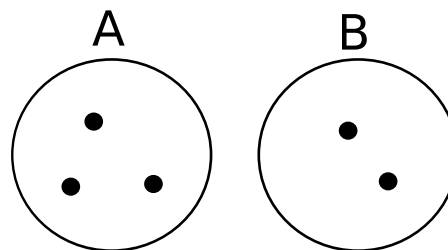
Inverslagar: $A \cup A^c = \mathcal{U}$
 $A \cap A^c = \emptyset$

Dominanslagar: $A \cap \emptyset = \emptyset$
 $A \cup \mathcal{U} = \mathcal{U}$

($A \cap B = B$ omm $B \subseteq A$)
($A \cup B = B$ omm $B \supseteq A$)

Om A, B disjunkta ($A \cap B = \emptyset$):

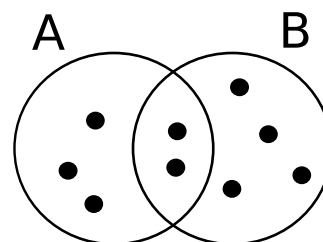
$$|A \cup B| = |A| + |B|$$



I allmänhet: (ej disjunkta eller disjunkta)

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

9
5
6
2



Exempel: Hur många tal x , $1 \leq x \leq 1000$ är delbara med minst en av 4 och 7?

$$\text{Låt } A = \{x \in \mathbb{N} \mid 1 \leq x \leq 1000, 4|x\} \quad |A| = \frac{1000}{4} = 250$$

$$B = \{x \in \mathbb{N} \mid 1 \leq x \leq 1000, 7|x\} \quad |B| = \left\lfloor \frac{1000}{7} \right\rfloor = 142$$

$$A \cap B = \{x \in \mathbb{N} \mid 1 \leq x \leq 1000, \text{mgm}(4; 7) = 28|x\}$$

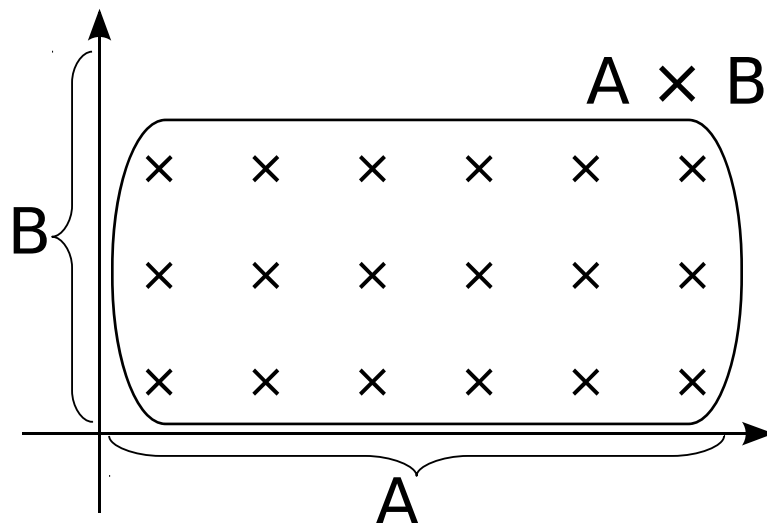
$$|A \cap B| = \left\lfloor \frac{1000}{28} \right\rfloor = 35$$

$$|A \cup B| = |A| + |B| - |A \cap B| = 250 + 142 - 35 = 357$$

Produktmängden:

$$A \times B = \{(a; b) \mid a \in A, b \in B\} \quad \times \text{ Kartesisk produkt}$$

Mängden av alla par med vänsterelement från A och högerelement från B .
 Paren är ordnade, $(a; b) \neq (b; a)$.



$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ — svarar mot punkter i planet

Induktionsbevis

För att visa ett påstående $P(n) \forall n \in \mathbb{N}$
räcker det att visa:

1) $P(0)$ bas (0 är lägsta talet i mängden)

$P(k) \Rightarrow P(k + 1) \quad \forall k \in \mathbb{N}$ steg

$$1 + 2 + \dots + n = \frac{n(n + 1)}{2}$$

2) För alla $k \in \mathbb{N}$

$(P(m) \forall m \in \mathbb{N}, m < k) \Rightarrow P(k)$

Ty: Antag att 1) eller 2) gäller, men $P(n)$ falskt för något $n \in \mathbb{N}$.

Då finns ett minst $n_0 \in \mathbb{N}$ med $P(n_0)$ falskt.

Fall 1) $n_0 = 0$?

Nej, $P(0)$ sann annars (basen) $n_0 = k + 1$, något $k \in \mathbb{N}$,
där $P(k)$ sann (m minst), steget ger $P(n_0)$ sann.

2) $P(m)$ sant för alla $m \in \mathbb{N}, m < n_0$ (n_0 minsta m , P falskt),
så $P(n_0)$ sann. Omöjligt i båda fallen så påståendet stämmer.

Rekursion

Exempel: På hur många olika sätt kan en $2 \times n$ gång läggas med 2×1 plattor?

Kalla antalet p_n .

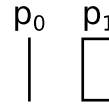
p_3  $p_3 = 3$

p_2  $p_2 = 2$

Svårt att finna en "formel", lätt med rekursion.

$$p_0 = p_1 = 1$$

$$p_2, p_3, p_4, p_5 = 2, 3, 5, 8$$



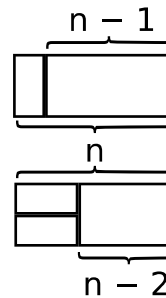
Man kommer fram till en funktion med hjälp av tidigare värden.

$$P_n = F_{n+1}, \quad F_n \text{ är Fibonaccitalen.}$$

$$F_0 = 0, \quad F_1 = 1$$

$$F_n = F_{n-1} + F_{n-2}, \quad n = 2, 3, \dots$$

steg



Rekursion: Om $G(n; f)$ är definierad för alla $n \in \mathbb{N}$ och $f: \{0, 1, \dots, n-1\} \rightarrow X$

så finns precis en funktion $f(n)$, $n \in \mathbb{N}$.

1)

$$\begin{cases} f(0) & \text{given} & \text{bas} \\ f(k+1) & \text{bestäms av } k, f(k) & \text{steg} \end{cases}$$

2)

$$f(n) = G(n; f) \geq 0, 1, \dots, n-1$$

Exempel: Visa med induktion att

$$P(n) : F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right)$$

Antag sant för $m < k$, visa att definitionen är sann för $m = k$

$$k = 0, 1, \dots$$

$$k = 2, 3, \dots$$

Om funktionen säger att $f : X \rightarrow Y$ (X och Y är mängder)
 Exakt en pil från varje $x \in X$. (Injektiv)

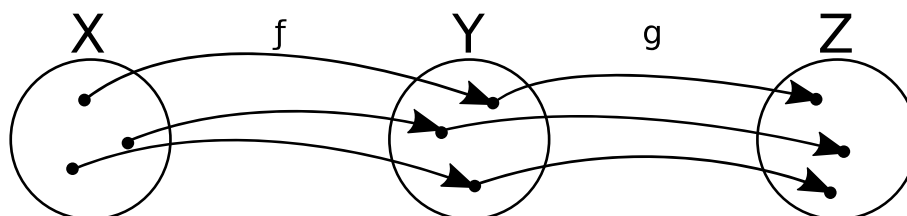
X är f:s domän, definitionsmängd
 Y är f:s kodomän, målmängd (värdemängd)

(ibland: $f = \{(x, f(x)) \mid x \in X\} \subseteq X \times Y$)

Sammansättning av funktioner (konkatenering, konkatination^{inkorrekt})

$f : X \rightarrow Y, \quad g : Y \rightarrow Z$

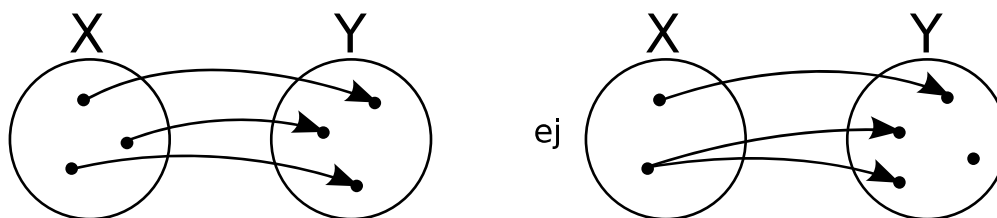
$g \circ f : X \rightarrow Z$ definieras av $(g \circ f)(x) = g(f(x))$
 (skrivs ibland (alltid av läraren), men bör inte skrivas, gf)



Viktiga typer av funktioner

Injektion: alla $y \in Y$ är bilder av högst ett $x \in X$

[\Leftrightarrow ekvivalent $y = f(x)$ högst en lösning $x \in X$
 för alla $y \in Y \Leftrightarrow (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$]



Surjektion:

Samma sak fast minst en istället för högst en.

Bijektion:

Exakt ett, med andra ord surjektion och injektion samtidigt.

Surjektion:

Givet $z \in Z$ så finns $y \in Y$ med

$z = g(y)$, men $y = f(x)$, något $x \in X$ (f surjektiv)

så $z = g(y) = g(f(x)) = (g \circ f)(x)$ så $g \circ f$ surjektiv.

2011-(02)feb-03: dag 6, 6

1) Ekvivalent: Finn x , k så att $16x - 42k = 26$

En linjär diofantisk ekvation.

Dividera med $z (= \text{sgd}(16; 42))$: $\mathbf{8}x - \mathbf{21}k = \underline{13}$

Euklides' algoritm:

$$\begin{array}{rcl} 21 & = & 2 \cdot 8 + 5 & (4) \\ 8 & = & 1 \cdot 5 + 3 & (3) \\ 5 & = & 1 \cdot 3 + 2 & (2) \\ 3 & = & 1 \cdot 2 + 1 & (1) \end{array}$$

Så:

$$\begin{array}{rcl} 1 & = & 3 - 2 = & (1) \\ & = & 3 - (5 - 3) = & (2) \\ & = & -5 + 2 \cdot 3 = & \\ & = & -5 + 2(\mathbf{8} - 5) = & (3) \\ & = & 2 \cdot \mathbf{8} - 3 \cdot 5 = & \\ & = & 2 \cdot \mathbf{8} - 3 \cdot (\mathbf{21} - 2 \cdot \mathbf{8}) = & (4) \\ & = & 8 \cdot \mathbf{8} - 3 \cdot \mathbf{21} & \end{array}$$

Så: $\underline{13} = 13 \cdot (8 \cdot \mathbf{8} - 3 \cdot \mathbf{21}) = \mathbf{8} \cdot (8 \cdot 13) + \mathbf{21} \cdot (-3 \cdot 13) =$
 $= \mathbf{8} \cdot 104 - \mathbf{21} \cdot 39$

Detta ger: $13 = 8x - 21k$
Skillnaden: $0 = 8(x - 104) - 21(k - 39)$
 $8(x - 104) = 21(k - 39)$

$$x - 104 = 21 \cdot c, \text{ något } c \in \mathbb{Z}$$

Så alla lösningar:

$$x = 104 + 21c = 20 + 21n \quad (21 \cdot 4 = 84)$$

Det vill säga:

Två lösningar: 20 och 41 i \mathbb{Z}_{42}

Ty: $\text{sgd}(16; 42) = 2$

$$2) \quad x \equiv 5 \pmod{8} \quad (1)$$

Innebär: $x/8 = k$, rest 5

Det första ger: $x = 5 + 8k \quad k \in \mathbb{Z}$

Den andra: $5 + 8k \equiv_{81} 73$

Det vill säga: $8k \equiv_{81} 68$

Som förra uppgiften, med Euklides' algoritm.

$$81 = 10 \cdot 8 + 1$$

$$1 = 81 \cdot 1 + 8(-10)$$

$$68 = 8(-680) + 81 \cdot 68$$

Så alla lösningar: $k = -680 + 81 \cdot m \quad m \in \mathbb{Z}$

Det vill säga: $k = 49 + 81 \cdot n \quad n \in \mathbb{Z}$

Alla lösningar, x , till (1):

$$x = 5 + 8(49 + 81n) = 397 + 648n$$

Om man ska lösa flera problem med samma moduler

finna d_1, d_2 så att

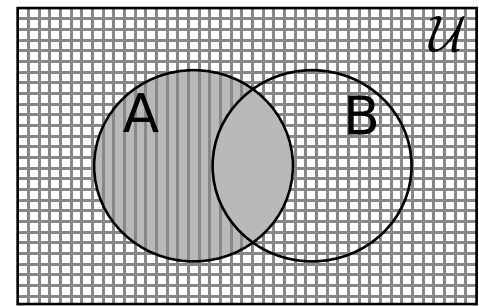
$$\begin{array}{lll} d_1 \equiv 1 \pmod{8} & \equiv 0 \pmod{81} \\ d_2 \equiv 1 \pmod{8} & \equiv 0 \pmod{81} \end{array}$$

3) Att visa: $((A^c \cup B^c) \setminus A)^c = A$ för godtyckliga mängder, A och B.

Med Venn-diagram:

Horisontella sträck: $A^c \cup B^c$
 Verticalla sträck: $(A^c \cup B^c) \setminus A$
 Grått: $((A^c \cup B^c) \setminus A)^c$

Alltså är $((A^c \cup B^c) \setminus A)^c = A$ ■



Med boolesk algebra:

$$\begin{aligned} ((A^c \cup B^c) \setminus A)^c &= \\ &= ((A^c \cup B^c) \cap A^c)^c = \\ &= (A^c \cup B^c)^c \cup A^{cc} = \\ &= (A^{cc} \cap B^{cc}) \cup A = \\ &= (A \cap B) \cup A = A \quad \blacksquare \end{aligned}$$

Andra sätt att visa detta på:

$$\begin{aligned} ((A^c \cup B^c) \setminus A)^c &\asymp \\ &\asymp \neg((\neg a \vee \neg b) \wedge \neg a) = \\ &= \neg(\neg(a \wedge b) \wedge \neg a) = \\ &= (a \wedge b) \vee a = a \quad \blacksquare \end{aligned}$$

$$\begin{aligned} ((A^c \cup B^c) \setminus A)^c &= \\ &= ((A^c \cup B^c) \cap A^c)^c = \\ &= ((A^c \cup B^c) \cap A^c)^c = \\ &= (A^c)^c = A \quad \blacksquare \end{aligned}$$

$$\begin{aligned} ((A^c \cup B^c) \setminus A)^c &= \\ &= ((A^c \cup B^c) \cap A^c)^c = \\ &= ((A \cap B)^c \cap A^c)^c = \\ &= ((A \cap B) \cup A) = A \quad \blacksquare \end{aligned}$$

(Fler liknande sätt finns)

4) Vi visar för en kvadrat med sidan $2k$

Induktion

Bas Påståendet sant då $k = 0$ inget
Kvar att täcka då en bit har tagits bort.

OK

Sats:

Antag sant för $k = p$ och betrakta kvadraten med sidan 2^{p+1} .

Dela upp den i fyra 2^p kvadrater tag bort en liten bit och en L-bit i mitten. Resten täcks av antagandet.

Så påståendet för $k = p \Rightarrow$ påståendet $k = p+1$

Induktionsprincipen

5) Fibonacci, rekursivt $F_0 = 0, \quad F_1 = 1$
 $F_{n+2} = F_n + F_{n+1}$

Visar med induktion

$$F_1^2 + F_2^2 + \dots + F_n^2 = F_n \cdot F_{n+1} \quad n = 1, 2, 3, \dots$$

$$\text{Bas: } VL = F_1^2 = 1 \quad HL = F_1 F_2 = 1 \cdot 1 = 1$$

Steg: Antag sant för $n = k$

$$VL_{k+1} = F_1^2 + F_2^2 + \dots + F_n^2 = F_n \cdot F_{n+1} = VL_k + F_{k+1}^2 = HL_k + F_{k+1}^2 =$$

$$= F_k F_{k+1} + F_{k+1}^2 = F_{k+1} (F_k + F_{k+1}) = F_{k+1} \cdot F_{k+2} = HL_{k+1}$$

$$\text{Så steget klart.} \quad VL_k = HL_k \Leftrightarrow VL_{k+1} = HL_{k+1}$$

b)

$$\text{Visa att } \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$$

$$\text{Bas: } VL_1 = \begin{pmatrix} F_2 & F_1 \\ F_1 & F_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^1 = HL_1$$

Antag sant för $n = k$

$$VL_{k+1} = \begin{pmatrix} F_{k+2} & F_{k+1} \\ F_{k+1} & F_k \end{pmatrix}, \quad HL_{k+1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{k+1}$$

$$VL_k \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_{k+1} + F_k & F_{k+1} \\ F_k + F_{k-1} & F_k \end{pmatrix} = \begin{pmatrix} F_{k+2} & F_{k+1} \\ F_{k+1} & F_k \end{pmatrix} = VL_{k+1}$$

6) Finn X, Y, Z , $f : X \rightarrow Y$, $g : Y \rightarrow Z$

Så att $g \circ f : X \rightarrow Z$ är bijektiv, men varken f , g bijektiv.

g måste vara en surjektion och
 f måste vara en injektion.

Så f inte surjektion och g inte injektion.

Om $X = Y = Z$ och f : injektion, inte surjektion, måste
 $X = Y$ var oändlig.

7) Givet $f : A \rightarrow A$, $f \circ f = \text{id}_A$ det vill säga $f(f(x)) = x \quad \forall x \in A$

Visa att f är bijektiv.

f är injektiv ty $f(x_1) = f(x_2) \Rightarrow f(f(x_1)) = f(f(x_2)) \Rightarrow x_1 = x_2$

f är surjektiv ty $x = f(f(x))$, $\forall x \in A$

Alltså f är bijektiv.

8) 2^{29} i bas 10 har 9 olika siffror, vilken siffra har 2^{29} inte?

$$(a_k a_{k-1} \dots a_1 a_0)_{10} \equiv_9 a_k + a_{k-1} + \dots + a_0$$

$$\text{Ty } a_n \cdot 10^n = a_n \underbrace{(999\dots 9 + 1)}_{\times n} \equiv_9 a_n$$

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0 \equiv_9 \text{???}$$

$$\begin{array}{lllll} 2^0 \equiv_9 1, & 2^1 \equiv_9 2, & 2^2 \equiv_9 4, & 2^3 \equiv_9 8, & 2^4 \equiv_9 7 \\ 2^5 \equiv_9 5, & 2^6 \equiv_9 1 & & & \end{array}$$

$$\text{Så } 2^{29} = 2^{6 \cdot 4 + 5} \equiv_9 1^4 \cdot 5 = 5$$

$$0 + 1 + 2 + \dots + 9 = 45 \equiv_9 0$$

$$2^{29}, \text{ siffersumma } \equiv_9 5$$

Om siffran x fattas så gäller

$$x + 5 \equiv_9 0$$

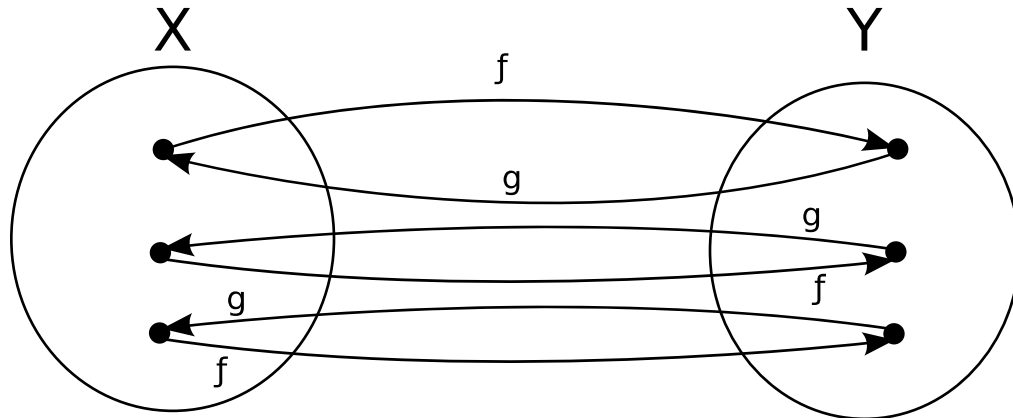
Så det är 4 som fattas.

2011-(02)feb-09: dag 7, 7

Först mer om funktioner

En inversfunktion till $f : X \rightarrow Y$ är en funktion $g : Y \rightarrow X$ så att

$$f \circ g = \text{id}_Y \text{ och } g \circ f = \text{id}_X \quad (\text{id}_Y(y) = y \text{ för alla } y \in Y)$$



Inversfunktionen skrivs f^{-1} .

f kallas invertabel (eller inverterbar) om f^{-1} existerar.

Om f är invertabel:

$$f(x_1) = f(x_2) \Rightarrow \underbrace{f^{-1}(f(x_1))}_{x_1} = \underbrace{f^{-1}(f(x_2))}_{x_2}$$

Så f injektiv.

För $y \in Y$ gäller $f(f^{-1}(y)) = y$, y godtyckligt, så f surjektiv.

Det vill säga f är en bijektion.

Och omvänt f bijektion:

$$\text{Definiera } g: \quad x = g(y) \Leftrightarrow y = f(x)$$

(“vänd pilarna”)

Sats: $f : X \rightarrow Y$ är invertabel omm den är en bijektion.

Man ser att om f, g är invertibla $\begin{cases} f : X \rightarrow Y \\ g : Y \rightarrow Z \end{cases}$

så är $g \circ f : X \rightarrow Z$ invertabel och $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Om X är ändlig och $f : X \rightarrow Y$ är en bijektion så är tydligen $|X| = |Y|$, de har samma kardinalitet. $|X| = n$ betyder att det finns en bijektion $f : \{1, 2, 3, \dots, n\} \rightarrow X$.

Också för oändliga mängder. Vi säger att X och Y har samma kardinalitet, $|X| = |Y|$ omm det finns en bijektion $f : X \rightarrow Y$.

Definition:

X är uppräknelig om det finns en bijektion $f : \mathbb{N} \rightarrow X$.

Observera att $\mathbb{N} = \{0, 1, 2, \dots\}$ är lika stor som $\mathbb{Z}_+ = \{1, 2, \dots\}$ ty en bijektion $f : \mathbb{N} \rightarrow \mathbb{Z}_+$ ges av $f(x) = x + 1$.

$$|\mathbb{N}| = |\mathbb{Z}_+|$$

Och $\mathbb{N} = A \cup B$, $A = \{0, 2, 4, \dots\}$, $B = \{1, 3, 5, \dots\}$

$A \cap B = \emptyset$ (disjunkta)

$$|A \cup B| = |A| = |B| > 0$$

$$|A| = |B| = |\mathbb{N}|$$

$$f(x) = x + 1 \quad g : \mathbb{N} \rightarrow A \quad g(x) = 2x$$

\mathbb{R} , de reella talen, är inte uppräknelig; den är överuppräknelig.

Ty: Antag att $f : \mathbb{N} \rightarrow \mathbb{R}$ är en bijektion.

$f(1) = \dots, \underline{a_{11}}a_{12}a_{13}\dots$ decimalbråk som inte slutar med 999... ($\overline{9}$)
 $f(2) = \dots, a_{21}\underline{a_{22}}a_{23}\dots$
 $f(3) = \dots, a_{31}a_{32}\underline{a_{33}}\dots$
 \vdots

Betrakta $x = 0, g(a_{11})g(a_{22})g(a_{33})$

$g(0) = 1$
 $g(d) = 0, \quad d = 1, 2, 3, \dots, 9$

då $x \neq f(n)$ för alla n ty olika n :e decimal.
 f inte surjektiv.

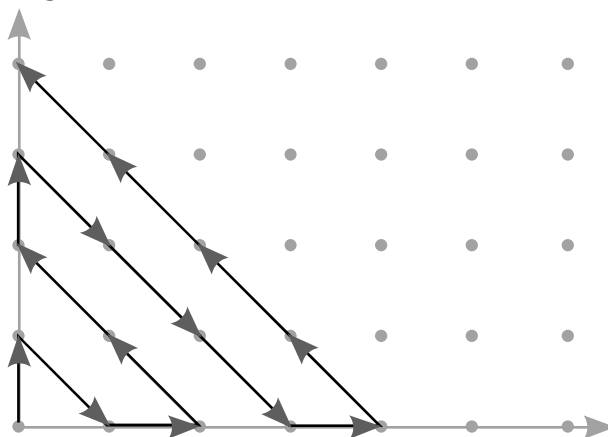
Motsägelse!

Men $|\mathbb{Q}| = |\mathbb{N}|$, de rationella tlen är uppräkneliga.

$$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$$

Oavsett vilken punkt
som väljs kommer den
kommas fram till.

$|X| < |Y|$ betyder att det finns en injektion
 $f : X \rightarrow Y$, men inte en surjektion.



Sats: $|A| < |\mathcal{P}(A)|$, alla mängder A .

Ty: Det finns en bijektion $g : A \rightarrow \mathcal{P}(A)$

$|X| < |Y|$: det finns en injektion $X \rightarrow Y$
det finns inte en bijektion.

$$g(a) = \{a\}$$

Låt $f : A \rightarrow \mathcal{P}(A)$. Vi ska se att f inte är en surjektion med
 $B = \{a \in A \mid a \notin f(a)\} \in \mathcal{P}(A)$.

För alla $a \in A$:	$a \in B \Leftrightarrow a \notin f(a)$	
Om $f(b) = B$:	$b \in B \Leftrightarrow b \notin f(b) = B$	Motsägelse!
$b \in A$:	f är inte surjektiv	

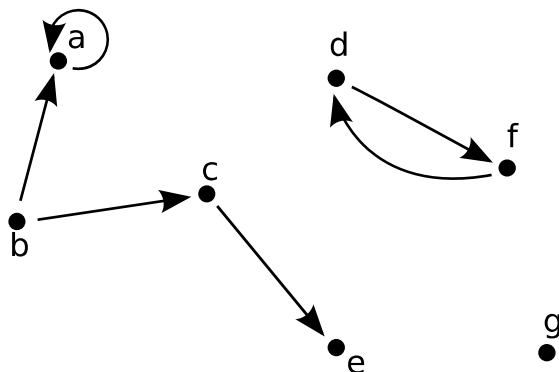
Binära relationer på en mängd \mathcal{R} en binär relation på mängden X
för alla $a, b \in X$ är $a \mathcal{R} b$ sant eller falskt.

Exempel: $\mid \leq < = \equiv_m \nmid$ på \mathbb{Z}
 $\subseteq \subset \mid A \mid = \mid B \mid A \cap B \neq \emptyset$ på mängder

Formellt definieras ofta

$$\mathcal{R} = \{(a, b) \in X^2 \mid a \mathcal{R} b\} \subseteq X^2 (= X \times X)$$

Beskrivs ibland med en graf



betyder $a \mathcal{R} b$ sant det vill säga
 $(a, b) \in \mathcal{R}$.

Kan också beskrivas med en matris

$$\begin{array}{c}
 \begin{array}{c} a \\ b \\ c \\ \vdots \end{array}
 \begin{array}{c} a \quad b \quad c \quad \dots \\ \left[\begin{array}{cccc} 1 & 0 & 0 & \dots \\ 1 & 0 & 1 & \dots \\ 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{array} \right] \end{array}
 \end{array}
 \quad x \mathcal{R} y \text{ om } 1 \text{ i position } xy$$

Viktiga egenskaper för binära relationer:

\mathcal{R} reflexiv:

$$\begin{array}{l}
 x \mathcal{R} x \quad \forall x \in X \\
 \text{exempel: } \quad | \quad \leq \quad = \quad \equiv_m
 \end{array}$$

\mathcal{R} symmetrisk:

$$\begin{array}{l}
 x \mathcal{R} y \Leftrightarrow y \mathcal{R} x \\
 \text{exempel: } \quad = \quad \equiv_m
 \end{array}$$

\mathcal{R} antisymmetrisk:

$$\begin{array}{l}
 x \mathcal{R} y, y \mathcal{R} x \Rightarrow x = y \\
 \text{exempel: } \quad \leq \quad \subseteq \quad |
 \end{array}$$

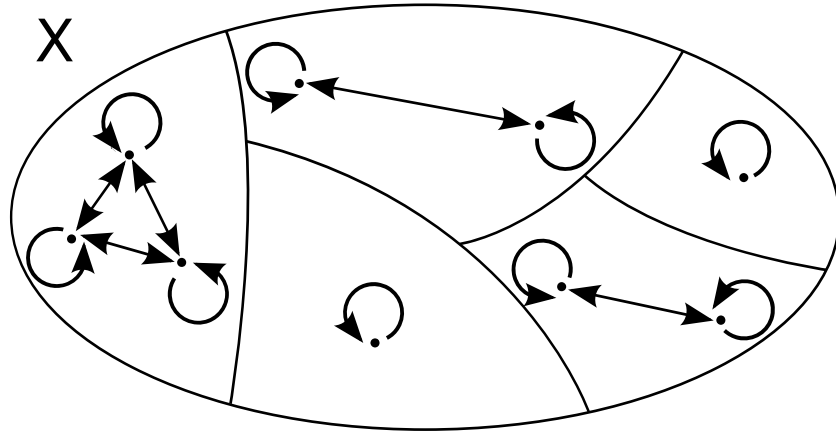
\mathcal{R} transitiv:

$$\begin{array}{l}
 x \mathcal{R} y, y \mathcal{R} z \Rightarrow x \mathcal{R} z \\
 \text{exempel: } \quad \geq \quad =
 \end{array}$$

\mathcal{R} kallas en ekvivalensrelation omm den är reflexiv, symmerisk och transitiv.

Exempel: $= \equiv_m \quad |\cdot| = |\cdot|$

En sådan delar X i ekvivalensklasser (disjunkta) $(y = \{x \in X \mid x \mathcal{R} y\})$

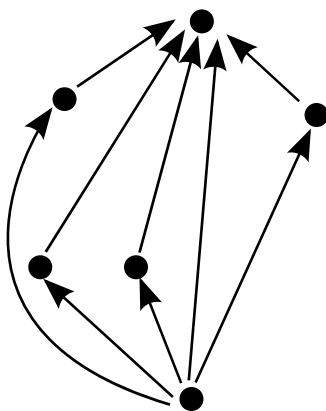


Ett exempel på en sådan är \equiv_m

\mathcal{R} kallas en partialordning omm den är reflexiv, antisymmetrisk och transitiv.

Exempel: \leq (för \mathbb{Z}) \subseteq (för $\mathcal{P}(Y)$) $|$ (för \mathbb{N})

$|$:



Inga cykler (sluta kurvor) av längen > 1 .

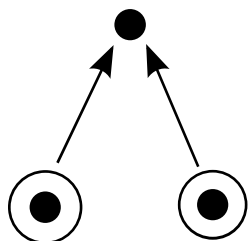
I samband med partialordning (\leq eller dylikt)

Ett element $a \in X$ (med partialordning \leq)
kallas minimalt om inget mindre:

$$x \leq a \Rightarrow x = a$$

Minst om det är mindre än alla:

$$a \leq x \quad \forall x \in X \quad (\text{likhet endast vid } x = a)$$



Minimal
det finns inget minsta

$a \text{ minst} \Rightarrow a \text{ minimalt}$
 $a \text{ minst} \not\Leftrightarrow a \text{ minimalt}$

På samma sätt; maximalt, störst.

Om $x \leq z$, $y \leq z$ är z en övre begränsning till X , Y
(Det finns även undre begränsning.)

Exempel: gemensam delare |.

Modul 2

2011-(02)feb-10: dag 1, 8

Dagens innehåll

Kombinatorik

Additionsprincipen

Lite om Ramseytal $r(s; t)$

Multiplikationsprincipen

Lite sannolikhet

$P(A \cup B)$ Om A, B disjunkt

$P(A \cup B)$ Allmänt

$P(A \cap B)$ Om A, B, oberoende

Betingade sannolikheten $P(A | B)$

Mer kombinatorik

Ordnat val med upprepning

Antalet funktion $f : X \rightarrow Y$

Ordnat val utan upprepning

Antalet injektioner $f : X \rightarrow Y$

Antalet permutationer av X (bijektioner $f : X \rightarrow X$)

Oordnat val utan upprepning

Binomialtalen $\binom{n}{k}$, Pascals triangel

Multinomialtalen $\binom{n}{k_1, k_2, \dots, k_m}$ eller $\binom{n}{k_1, k_2, \dots, k_m}$

Kombinatorik; att räkna "saker" (antalet element i mängder)

Additionsprincipen:

Om A, B är ändliga och disjunktiona ($A \cap B = \emptyset$)

$$\text{så } |A \cup B| = |A| + |B|.$$

(Kan visas med induktion över $\underbrace{\text{antalet element över } B}_{|B|}$ (r över n)

Med induktion:

$$|A_1 \cup \dots \cup A_m| = |A_1| + \dots + |A_n| \text{ om } A_i \cap A_j = \emptyset \forall i \neq j$$

Exempel:

En klass har 12 pojkar och 11 flickor. Hur många barn i klassen?

Låt $A = \{\text{pojkar}\}$, $B = \{\text{flickor}\}$

$$|A \cup B| = |A| + |B| = 12 + 11 = 23$$

Förutsatt att varje barn är antligen pojke eller flicka (har exakt ett kön).

Exempel:

Bland 6 personer finns måste det finns 3 som alla känner varandra eller 3 som inte känner varandra.

Ty: Betrakta en person, Lisa (L).

Övriga fem delas in i två delar:

A: De som L känner

B: De som L inte känner

$A \cap B = \emptyset$, $|A \cup B| = 5 = \{\text{additionsprincipen}\} = |A| + |B|$
så $|A| \geq 3$ eller $|B| \geq 3$.

1) Om $|A| \geq 3$:

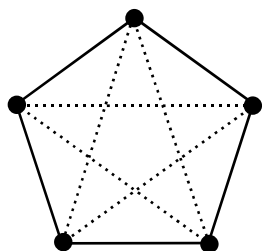
Om två i A känner varandra, de u {L} känner alla varandra.
3 st, annars $|A| \geq 3$, ingen känner varandra.

2) Om $|B| \geq 3$:

På samma sätt.

Skulle det räcka med 5 personer?

Nej



Allmänt:

Låt $r(s; t)$ vara minsta antalet personer så att det säkert finns
5 personer som alla känner varandra eller t personer som inte
känner varandra.

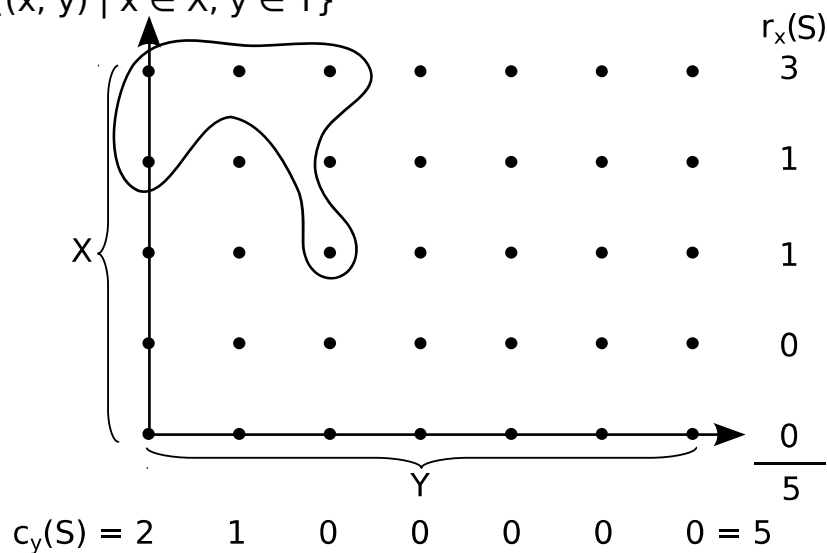
Vi har visat att $r(3; 3) = 6$

Svåra att finna

Ramsey

$r(2; t) = t$

Om X, Y är mängder, $X \times Y = \{(x; y) \mid x \in X, y \in Y\}$



Sats: Om $S \subseteq X \times Y$, X, Y ändliga

$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} c_y(S)$$

$$\begin{aligned} \text{där } r_x(S) &= |\{y \in Y \mid (x; y) \in S\}| \\ c_y(S) &= |\{x \in X \mid (x; y) \in S\}| \end{aligned}$$

Speciellt:

$$S = X \times Y \quad |X \times Y| = |X| \cdot |Y| \quad (\text{multiplikationsprincipen})$$

Exempel:

Hur många stavelser (Konsonant(C) — Vokal(V)) finns i svenskan?

$$|\{\text{ba, be, bi, ..., zå, zä, zö}\}| = |C \times V| = |C| \cdot |V| = 19 \cdot 9 = 171 \text{ st}$$

Exempel:

I en klass finns 32 pojkar. Varje pojke känner 5 flickor i klassen och varje flicka känner 8 pojkar.

Hur många flickor finns i klassen.

Låt $X = \{\text{flickorna}\}$, $Y = \{\text{pojkarna}\}$

$S \subseteq X \times Y$, $S = \{(x; y) \in X \times Y \mid x \text{ och } y \text{ känner varandra}\}$

$$\begin{aligned} \text{Då } r_x(S) &= \text{antalet pojkar } x \text{ känner} = 8 & \text{alla } x \\ c_y(S) &= \text{antalet flickor } y \text{ känner} = 5 & \text{alla } y \end{aligned}$$

$$|S| = \begin{cases} \sum_{x \in X} r_x(S) = 8 \cdot |X| \\ \sum_{y \in Y} c_y(S) = 5 \cdot |Y| = 5 \cdot 32 = 160 \end{cases}$$

$$\text{Så } |X| = 20 \quad \because \quad 160/8 = 20$$

Lite om sannolikheter

Om vi har ett ändligt utfallsrum (alla elementarhändelser), Ω , där varje element är lika sannolikt ("likafördelning"), så har händelen $A \subseteq \Omega$.

$$\text{Sannolikheten } P(A) = \frac{|A|}{|\Omega|}$$

Exempel: Vad är sannolikheten för 1 krona(1) och 1 klave(0) då ett mynt singlar 2 gånger?

1) Utfallen $\Omega = \{00, 01, 10, 11\}$

En av varje: $A = \{01, 10\}$

$$P(A) = \frac{|A|}{|\Omega|} = \frac{2}{4} = \frac{1}{2}$$

2) Utfallen $\Omega = \{11, 00, (1 \text{ av varje } (01 \text{ eller } 10))\}$

$A = \{1 \text{ av varje}\}$

$$P(A) = \frac{|A|}{|\Omega|} = \frac{1}{3}$$

2) är felaktig eftersom händelserna inte är lika sannolika.

Händelser A, B kallas oberoende om $P(A \cap B) = P(A) \cdot P(B)$.

Om A, B är disjunkta: $(A \cap B = \emptyset)$
 $P(A \cup B) = P(A) + P(B)$.

Om X, Y är (ändliga) mängder,
 $|X| = m, |Y| = n$:

Sats: Antalet funktioner $f : X \rightarrow Y$ är $n^m = |Y|^{|X|} =$

$=$ antalet element i $Y^m = \underbrace{Y \times \dots \times Y}_{\times m} =$

$=$ antalet ord av längden m , alfabet $Y =$

$=$ antalet ordnade val av m stycken ur Y med upprepning

“Ordnat val med upprepning”

Exempel: Hur många ord av längden m finns i alfabetet $\{a, b, c, d, e\}$?

Enligt ovan: 5^m stycken

Hur många av dem innehåller 'b'?

Jo, alla utom de som *inte* innehåller 'b':
 $5^m - 4^m$ (additionsprincipen)

Nästa fall:

Sats: Antalet injektioner $f : X \rightarrow Y$ = antalet ord av längden m , alfabetet Y , utan upprepning =
= antalet ord, ordnade val av m stycken ur Y utan upprepning =

$$= \underbrace{n(n-1)(n-2)\cdots(n-m+1)}_{\times m} = (n)_m = \frac{n!}{(n-m)!}$$

Multiplikationsprinzipien

“Ordnat val utan upprepning”

Exempel: Hur många injektioner $\{1, 2, 3, 4\} \rightarrow \{1, 2, \dots, 6\}$ finns?

Som i satsen $(m = 4, n = 6) : (6)_4 = 6 \cdot 5 \cdot 4 \cdot 3 = 360$

Hur många av dem tar värdet 3?

Jo, alla utom dem som inte gör det.

$$(6)_4 - (5)_4 = 360 - 5 \cdot 4 \cdot 3 \cdot 2 = 360 - 120 = 240 \text{ stycken}$$

Alternativt:

$$4 \cdot \underbrace{5 \cdot 4 \cdot 3}_{\text{övriga}} = 240$$

3:ans position

Speciellt: Om $X = Y$ (ändliga), injektioner blir bijektioner, permutationer?

$m = n$ så antalet

$$\begin{aligned} n(n-1)(n-2)\cdots(n-m+1) &= \\ &= n(n-1)(n-2)\cdots 1 = n! \end{aligned}$$

$$|X| = n$$

Tredje fallet:

Oordnade urval utan upprepning

Låt X vara en n -mängd, det vill säga $|X| = n$.

Definiera: Antalet oordnade val av k stycket från X , utan upprepning.

Binomialtalet $\binom{n}{k}$ "n över k"

Exempel:

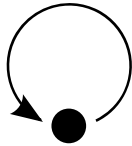
$$\binom{5}{3} = 10, \text{ ty alla 3-delmängder till } \{a, b, c, d, e\} \text{ ges av}$$

abc, abd, abe, acd, ace,
ade, bcd, bce, bde, cde.

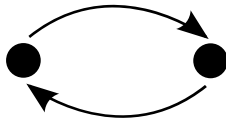
2011-(02)feb-10: dag 2, 9

1a)

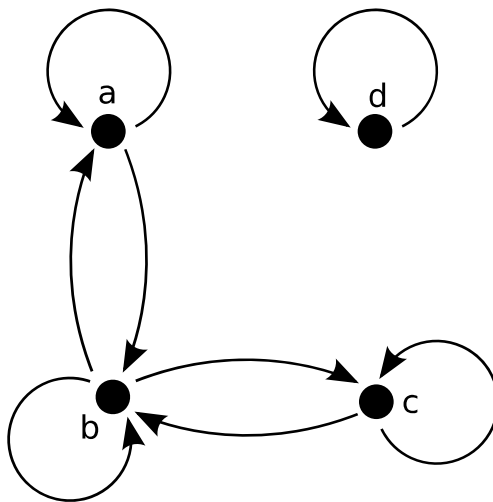
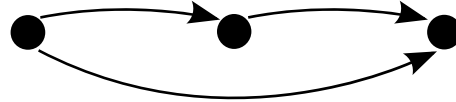
Reflexiv



Symmetrisk



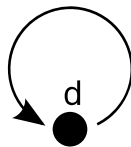
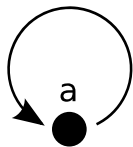
Transitiv



$\mathcal{R} = \{(a; a), (b; b), (c; c), (d; d), (a; b), (b; a), (b; c), (c; b)\}$

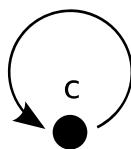
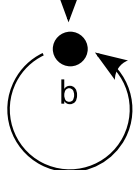
Inte transitiv ty $a\mathcal{R}b$, $b\mathcal{R}c$, men inte $a\mathcal{R}c$.

b)



$\mathcal{R} = \{(a; a), (b; b), (c; c), (d; d), (a; b)\}$

Transitiv ty $x\mathcal{R}y$ och $y\mathcal{R}z \Rightarrow x\mathcal{R}z$.
(uppstår om $x = y = z$ eller om $x = y = a, z = b$)



c)

$\mathcal{R} = \emptyset$

Icke-reflexiv, symmetrisk och transitiv.

- 2) A är en mängd. Vilka binära relationer är både ekvivalensrelationen och partialordningen?

Ekvivalensrelationen:

$$\begin{array}{llll} \text{Reflexiv,} & \text{symmetrisk,} & \text{transitiv} & \\ xRx & xRy \Rightarrow yRx & xRy \wedge yRz \Rightarrow xRz & \forall x, y, z \in A \end{array}$$

Partialordningen:

$$\begin{array}{llll} \text{Reflexiv} & \text{antisymmetrisk} & \text{transitiv} & \\ xRx & xRy \wedge yRx \Rightarrow x = y & xRy \wedge yRz \Rightarrow xRz & \forall x, y, z \in A \end{array}$$

Låt aRb då bRa (symmetrisk) så $a = b$ (antisymmetrisk)
och $a = b \Rightarrow aRb$ (reflexiv) så $aRb \Leftrightarrow a = b$,
så likhet är enda (eventuellt möjliga),
men = relationen är reflexiv, symmetrisk, antisymmetrisk och transitiv.
Så enda möjliga relationen är likhetsrelationen.

Ekvivalensklasser: $[x] = \{y \mid y \in A, y R x\}$
 $[x] = \{x\}$

3)

$$\begin{aligned} 2646000 &= 2645 \cdot 2^3 \cdot 5^3 = 2^4 \cdot 5^3 \cdot 3^3 \cdot 7^2 \\ &\quad \swarrow \\ &= 2 \cdot 1323 = 2 \cdot 3 \cdot 441 = 2 \cdot 3^2 \cdot 147 = \\ &= 2 \cdot 3^3 \cdot 49 = 2 \cdot 3^3 \cdot 7^2 \end{aligned}$$

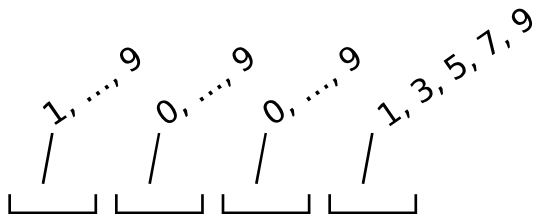
Varje delare har formen $2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot 7^{e_4}$,
med $0 \leq e_1 \leq 4$, $0 \leq e_2, e_3 \leq 3$, $0 \leq e_4 \leq 2$.

Alla olika e ger olika delare.

Multiplicationsprincipen:

Svar: $5 \cdot 4 \cdot 4 \cdot 3 = 240$ delare.

4)



Svar: $9 \cdot 9 \cdot 8 \cdot ?$

Istället $5 \cdot 8 \cdot 8 \cdot 7 = 2240$ stycken.

Ental Tusental

5)

Sökta antalet = totala antalet – antalet
sätt med L och O brevid varandra =

$$= 13! - 2 \cdot 13 \cdot 11! =$$

LO Vilken stol sitter L på
OL Övriga 11 persner på övriga stolar.

$$= 13 \cdot 10 \cdot 11! = \text{Massor!}$$

Sats:

$$\binom{n}{0} = \binom{n}{n} = 1 \quad \forall n \geq 0$$

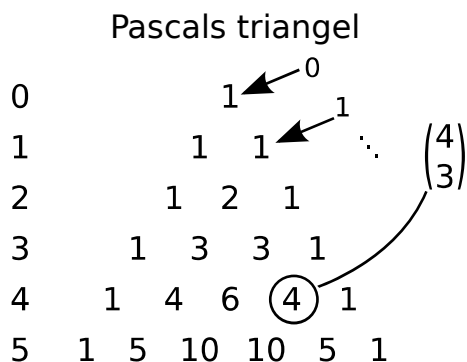
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \quad \text{om } 0 < k < n$$

Välj ut $x_0 \in X$ (n-mängd)

$$\binom{n}{k} = \text{antalet } k\text{-mängder till } X = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Exempel:

$$\binom{4}{3} = \binom{3}{2} + \binom{3}{3} = \binom{2}{1} + \binom{2}{2} + 1 = \binom{1}{0} + \binom{1}{1} + 1 + 1 = 4$$



Sats:

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

Binominalsatsen:

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

7a) Additionsprincipen

$$\binom{15}{2} \binom{11}{3} + \binom{15}{3} \binom{11}{2} + \binom{15}{4} \binom{11}{1} = \dots = 57365 \text{ sätt}$$

b) Totala antalet – specifika antalet

Specifika $\binom{14}{1} \binom{10}{2} + \binom{14}{2} \binom{10}{1} + \binom{14}{3} \binom{10}{0}$

eller $\binom{24}{3} - \binom{14}{0} \binom{10}{3} = 1904$

$$57365 - 1904 = 55461$$

2011-(02)feb-17: dag 3, 10

Mer kombinatorik

Exempel från övning 3

Oordnat val utan upprepning avslutning

Multinomial tal $\binom{n}{k_1, k_2, \dots, k_m}$

Oordnat val med upprepning

k stycken oordnade valda från en n-mängd.

$\binom{n + k - 1}{k}$ sätt

Postfacksprincipen

Ingen injektion $f : X \rightarrow Y$ om $|X| > |Y|$

Genererande funktion

Från övning 3:

9) Visa att för $n \in \mathbb{N}$ gäller att

$$\frac{1}{1} \binom{n}{0} + \frac{1}{2} \binom{n}{1} + \dots + \frac{1}{n+1} \binom{n}{n} = \frac{2^{n+1} - 1}{n+1}$$

Binomialsatsen ger

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

Tag $\int_0^1 \dots dt$ av båda leden:

$$\left[\frac{(1+t)^{n+1}}{n+1} \right]_0^1 = \sum_{k=0}^n \binom{n}{k} \left[\frac{t^{k+1}}{k+1} \right]_0^1$$

Det vill säga

$$\frac{2^{n+1}}{n+1} - \frac{1}{n+1} = \sum_{k=0}^n \frac{1}{k+1} \binom{n}{k} \quad \text{Det vi ville visa.}$$

Alternativt:

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

10) Finn för $n \in \mathbb{N}$

$$\binom{n}{0} + \binom{n-1}{n} + \binom{n-2}{2} + \dots + \binom{n - \lfloor n/2 \rfloor}{\lfloor n/2 \rfloor} = \sum_{k=-\infty}^{\infty} \binom{n-k}{k}$$

$$n = 0: \quad \binom{0}{0} = 1$$

$$n = 1: \quad \binom{1}{0} = 1$$

$$n = 2: \quad \binom{2}{0} + \binom{1}{1} = 2$$

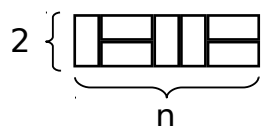
$$n = 3: \quad \binom{3}{0} + \binom{2}{1} = 3$$


$$n = 4: \quad \binom{4}{0} + \binom{3}{1} + \binom{2}{2} = 5$$



$$n = 5: \quad \binom{5}{0} + \binom{4}{1} + \binom{3}{2} = 8$$


Kombinatoriskt:

F_{n+1} = Antalet sätt att plattläga en $2 \times n$ -gång med 2×1 -plattor.



Antalet sätt att göra det med precis k stycken 

är $\binom{n-k}{k}$ ← Antalet pos för  eller 

← Antalet pos med 

Lite till om oordnade urval utan upprepning

Exempel:

186 studenter skall fördelas på 4 övningsgrupper med 36, 42, 45 respektive 63 platser. Hur många sätt är möjliga?

Multiplikationsprincipen:

$$\binom{186}{36} \binom{186 - 36 = 150}{42} \binom{150 - 42 = 108}{45} \binom{63}{63} =$$

Grupp 2
Antalet sätt att fylla grupp 1.

$$= \frac{186!}{36!(186 - 36)!} \cdot \frac{150!}{42!108!} \cdot \frac{108!}{45!63!} \cdot \frac{63!}{63!0!} =$$
$$= \frac{186!}{36! 42! 45! 63!} = \binom{186}{36, 42, 45, 63}$$

Multinomialtal:

$$\binom{n}{k_1, k_2, \dots, k_m}, \quad k_i \geq 0, \quad \sum k = n$$

Ger antalet sätt att fördela n särskiljbara element i m särskiljbara lådor med k_i element i låda "i" = antalet funktion $f: X \rightarrow Y$, där värdet "i" antas precis k_i gånger.

m-mängd n-mängd

Sats:

$$\binom{n}{k_1, k_2, \dots, k_m} = \frac{n!}{k_1! k_2! \dots k_m!} \quad \left(\binom{n}{k} = \binom{n}{k, n-k} \right)$$

$$(x_1 + x_2 + \dots + x_m)^n = \sum_{\substack{k_i \in \mathbb{N} \\ \sum k = n}} \binom{n}{k_1, \dots, k_m} = x_1^{k_1} \dots x_m^{k_m}$$

$$\begin{aligned} \binom{n}{k_1, k_2, \dots, k_m} &= \binom{n-1}{k_1-1, k_2, \dots, k_m} + \\ &+ \binom{n-1}{k_1, k_2-1, \dots, k_m} + \dots + \binom{n-1}{k_1, k_2, \dots, k_m-1} \end{aligned}$$

$$\binom{n}{0, k_2, \dots, k_m} = \binom{n}{k_2, \dots, k_m}$$

Exempel:

Vad är koefficienten för $x^3 y^5 z^{12}$ i $(x + y + z)^{20}$?

Jo, den är (enligt multinomialsatsen)

$$\binom{20}{3, 5, 12} = \frac{20 \cdot 19 \cdot \dots \cdot 14 \cdot 13}{1 \cdot 2 \cdot 3 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = \dots = 7054320$$

Exempel:

Hur många ord kan man bilda med omkastning av bokstäverna i ordet "vetekatt"?

Jo, antalet funktion från positionerna (8 stycket) till $\{a, e, k, t, v\}$.

Med 1:a, 2:a, ...

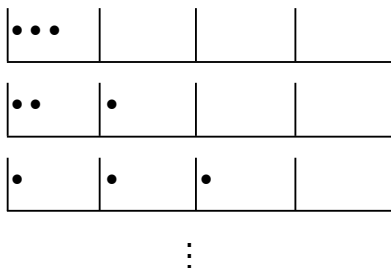
$$\binom{8}{1, 2, 1, 3, 1} = \frac{8!}{1! 2! 1! 3! 1!} = \frac{8!}{2! 3!} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{2} = 3360 \text{ stycken}$$

Fjärde urvalsfallet

Exempel:

På hur många sätt kan 3 identiska kulor placeras i 4 (särskiljbara) lådor?
Oordnat val med upprepning. (Eventuellt flera kulor i samma låda.)

aaa acc bcd
aab acd bdd
aac add ccc
aad bbb ccd
abb bbc cdd
abc bbd ddd
abd bcc



Totalt 20 stycken.

Allmänt:

Antalet oordnade val av k stycken från en k -mängd med upprepning =
 antalet sätt att skriva $k = x_1 + x_2 + \dots + x_n =$ $x_i \geq 0$

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

.....

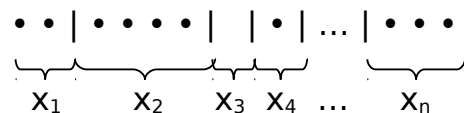
Exempel:

$$k = 3, n = 4$$

$$\binom{4 + 3 - 1}{3} = \binom{6}{3} = \frac{6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3} = 20$$

Ty:

$k = x_1 + x_2 + \dots + x_n$ kan bijektivt skrivas



Antalet symboler (\bullet och $|$) =
 $= n + k + 1$

Varje svarar precis mot val av vilka k stycken som ska vara " \bullet ",
 resten är " $|$ ".

Exempel:

En befolkning på 4711 personer skall rösta bland 8 partier (inklusive ogiltiga och avstått). Hur många möjliga valresultat?

Jo, antalet heltalslösningar till

$$\begin{aligned} 4711 &= x_1 + \dots + x_8 = \\ &= \binom{4711 + 8 - 1}{8 - 1} = \binom{4711 + 8 - 1}{7} = \dots \approx 1,03 \cdot 10^{22} \end{aligned}$$

Postfacksprincipen

Sats: Om $|X| > |Y|$ finns ingen injektion $f : X \rightarrow Y$.
"Om n saker läggs i m lådor, $n > m$, blir det minst 2 saker i minst en låda."

Exempel: Bland 367 personer finns alltid 2 med samma födelsedag.

Exempel: Pelle äter minst en glass om dagen under 11 veckor, aldrig mer än 12 glassar under en vecka. Visa att det finns en följd dagar då han äter exakt 21 glassar.

Låt a_i vara totala antalet glass han äter de första " i " dagarna.

$$1 \leq a_1 < a_2 < \dots < a_{77} \leq 11 \cdot 12 = 132 \quad \text{och låt } b_i = a_i + 21$$

$$22 \leq b_1 < b_2 < \dots < b_{77} \leq 132 + 21 = 153$$

Så de 154 talen a_i, b_j finns bland $\{1, 2, \dots, 153\}$ så minst två lika.

Alla a_i olika, alla b_j olika, så $a_i = b_j$, några i, j .

Det vill säga $a_i = a_j + 21$, så han äter precis 21 glassar under dagarna $j + 1, j + 2, \dots, i$.

2011-(02)feb-24: dag 4, 11

Mer kombinatorik

Genererande funktioner

Ett exempel

Principen om inklusion/exklusion (sällprincipen)

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

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

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \dots + (-1)^{n+1} \alpha_n$$

$$\text{där } \alpha_i = \sum_{1 \leq k_1 < \dots < k_i \leq n} (A_{k_1} \cap \dots \cap A_{k_i})$$

Uppdelning av mängder

Stirlingtal (av andra slaget) $S(n; k)$

Antalet surjektioner $f : X \rightarrow Y$

Partitioner av partial tal

Först om genererande funktioner.
(för att studera talföljder)

Exempel:

$$\begin{cases} F_0 = 0, F_1 = 1 \\ F_{n+2} = F_{n+1} + F_n, \quad n = 0, 1, 2, \dots \end{cases}$$

Deras genererande funktion:

$$g(x) = \sum_{n=0}^{\infty} F_n x^n$$

Tag rekursiva ekvationen och multiplicera med x^{n+2} och $\sum_{n=1}^{\infty}$

$$\underbrace{F_2 x^2 + F_3 x^3 + \dots}_{g(x) - F_1 x - F_0} = \underbrace{F_1 x^2 + F_2 x^3 + \dots}_{x(g(x) - F_0)} + \underbrace{F_0 x^2 + F_1 x^3 + \dots}_{x^2 \cdot g(x)}$$

$$(x^2 + x - 1) g(x) = -x$$

så

$$g(x) = \frac{-x}{x^2 + x - 1} =$$

$$= \left\{ \begin{array}{l} \psi = -\frac{1}{\phi} = \\ = -1 - \phi \\ \phi - \psi = \sqrt{5} \end{array} \left| \begin{array}{l} x^2 + x - 1 = 0 \\ x = -\frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{-1 \pm \sqrt{5}}{2} \\ \phi = \frac{\sqrt{5} - 1}{2} \approx 0,618 \\ \phi = \frac{\sqrt{5} + 1}{2} \approx 1,618 \end{array} \right. \right\} =$$

$$= \frac{-x}{(x - \phi)(x - \psi)} =$$

$$\begin{aligned}
&= \frac{\left(\frac{-\phi}{\phi - \psi}\right)}{x - \phi} + \frac{\left(\frac{-\psi}{\psi - \phi}\right)}{x - \psi} = \\
&= \frac{\left(\frac{1}{\phi - \psi}\right)}{1 - \frac{x}{\phi}} + \frac{\left(\frac{1}{\psi - \phi}\right)}{1 - \frac{x}{\psi}} = \\
&= \frac{1}{\sqrt{5}} \left(\frac{1}{1 + \psi x} - \frac{1}{1 + \phi x} \right) = \\
&= \frac{1}{\sqrt{5}} \left(\sum_{n=0}^{\infty} (-\psi)^n x^n - \sum_{n=0}^{\infty} (-\phi)^n x^n \right)
\end{aligned}$$

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

F_n är koefficient för x^n :

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right)$$

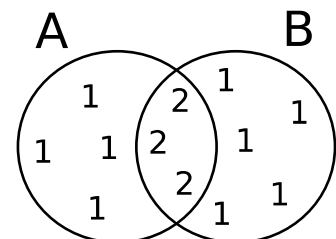
Principen om exklusion/inklusion (sällprincipen)

Additionsprincipen:

$$|A \cup B| = |A| + |B| \text{ om } A \cap B = \emptyset$$

Mer allmänt:

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

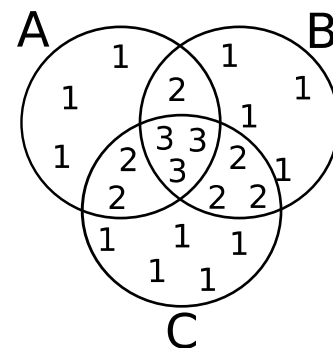


För tre mängder:

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

Exempel:

I en klass med 47 elever tycker i mängden B om bullar 25 stycken; G om glass, 20 stycken; och T om tårta 19 stycken.



B och G: 8 stycken
 B och T: 12 stycken
 G och T: 5 stycken
 Alla tre: 1 styck

Hur många i klassen tycker inte om någondera?

$$|B \cup G \cup T| = |B|_{25} + |G|_{20} + |T|_{19} - |B \cap G|_8 - |B \cap T|_{12} - |G \cap T|_5 + |B \cap G \cap T|_1 = 40$$

Resten, de sökta: 7 stycken.

Allmänt: (A_i ändliga)

Sats:

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= |A_1| + \dots + |A_n| - \\ &\quad - (|A_1 \cap A_2| + \dots + |A_1 \cap A_n| + |A_2 \cap A_3| + \dots + \\ &\quad + |A_2 \cap A_n| + \dots + |A_{n-1} \cap A_n|) + \dots + (-1)^{n+1} |A_1 \cap \dots \cap A_n| = \\ &= \alpha_1 - \alpha_2 + \alpha_3 - \dots + (-1)^{n+1} \alpha_n \\ \text{där } \alpha_i &= \sum_{1 \leq k_1 < \dots < k_i \leq n} (A_{k_1} \cap \dots \cap A_{k_i}) \end{aligned}$$

Bevis:

Låt x ingå i precis k stycken av $A_1 \dots A_n$.
Hur många gånger räknas det?

$$\begin{aligned} \text{Jo, } k - \binom{k}{2} + \binom{k}{3} - \dots + (-1)^{k+1} \binom{k}{k} &= \\ &= 1 - \left(\binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \dots + (-1)^k \binom{k}{k} \right) = \\ &= 1 - (1 - 1)^k = \begin{cases} 0 & k = 0 \\ 1 & k = 1, 2, \dots \end{cases} \end{aligned}$$

Exempel:

n personer tar i tumult en hatt var. Vad är sannolikheten att någon får sin egen hatt?

("I tumult": lika fördelat i $S_n = \{\text{bijektioner av } \{1, 2, \dots, n\}\}$)

Sökta sannolikheten:

$$P = \frac{1}{|S_n|} |\{f \in S_n : f(i) \neq i \text{ alla } i = 1, 2, \dots, n\}|$$

$$\text{Låt } A_i = \{f \in S_n \mid f(i) = i\}, \quad |A_i| = (n-1)!$$

$$P = \frac{1}{n!} (|S_n| - |A_1 \cup \dots \cup A_n|) =$$

$$= \frac{1}{n!} (n! - [|A_1| + \dots + |A_n| - (|A_1 \cap A_2| + \dots) + (|A_1 \cap A_2 \cap A_3| + \dots) + \dots]) =$$

$$= \frac{1}{n!} \left(n \cdot (n-1)! + \binom{n}{2} (n-2)! - \binom{n}{3} (n-3)! + \dots + (-1)^n \binom{n}{n} (n-n)! \right) =$$

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

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

$$= \left\{ \frac{n!}{k!} = \frac{1}{k'!}, k' = n - k \right\} =$$

$$= \sum_{k=0}^n (-1)^k \frac{1}{k!} \approx e^{-1},$$

$$\text{fel: } \frac{(-1)^{n+1}}{(n+1)!} e^{\xi}, \quad -1 < \xi < 0$$

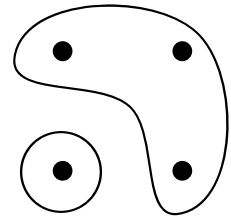
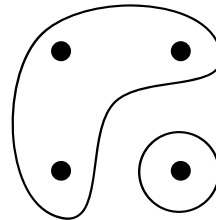
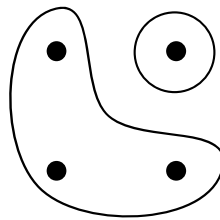
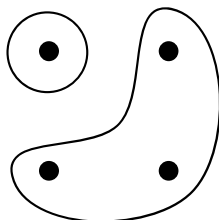
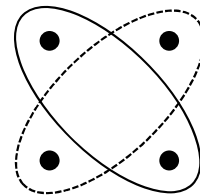
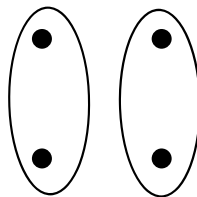
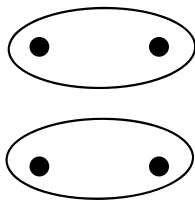
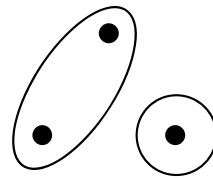
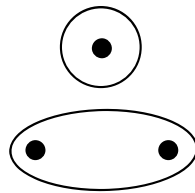
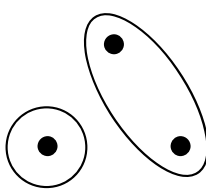
Uppdelning av mängder

Definition:

Stirlingtalen (av 2:a slaget)

$S(n; k)$ är antalet uppdelningar av en n -mängd (särskiljbara element) i k (särskiljbara) högar ($\neq \emptyset$).

Exempel: $S(3; 2) = 3$
 $S(4; 2) = 7$



Sats:

$$\begin{cases} S(n; k) = S(n-1; k-1) + k \cdot S(n-1; k) & 1 < k < n \\ S(n; 1) = S(n; n) - 1 & n \geq 1 \end{cases}$$

Ty: (rad 2 klart)

rad 1:

Välj ett element x_0 . Då finns 2 typer av uppdelningar:

- 1) x_0 ensam i sin hög.
 $S(n - 1; k - 1)$ stycken.
- 2) x_0 med andra, alla övriga kan fördelas på
 $S(n - 1; k)$ sätt och x_0 's hög kan väljas på k sätt.

$S(n; k)$ kan sättas in i "Stirlings triangel".

n:

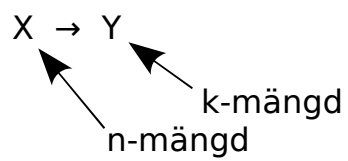
k:

n \ k	0	1	2	3	4	5	6	7
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	6	6	4	1			
5	1	10	10	6	4	1		
6	1	15	15	10	6	4	1	
7	1	21	21	14	10	6	4	1

Större tabell på Wikipedia:

http://en.wikipedia.org/wiki/Stirling_numbers_of_the_second_kind#Table_of_values

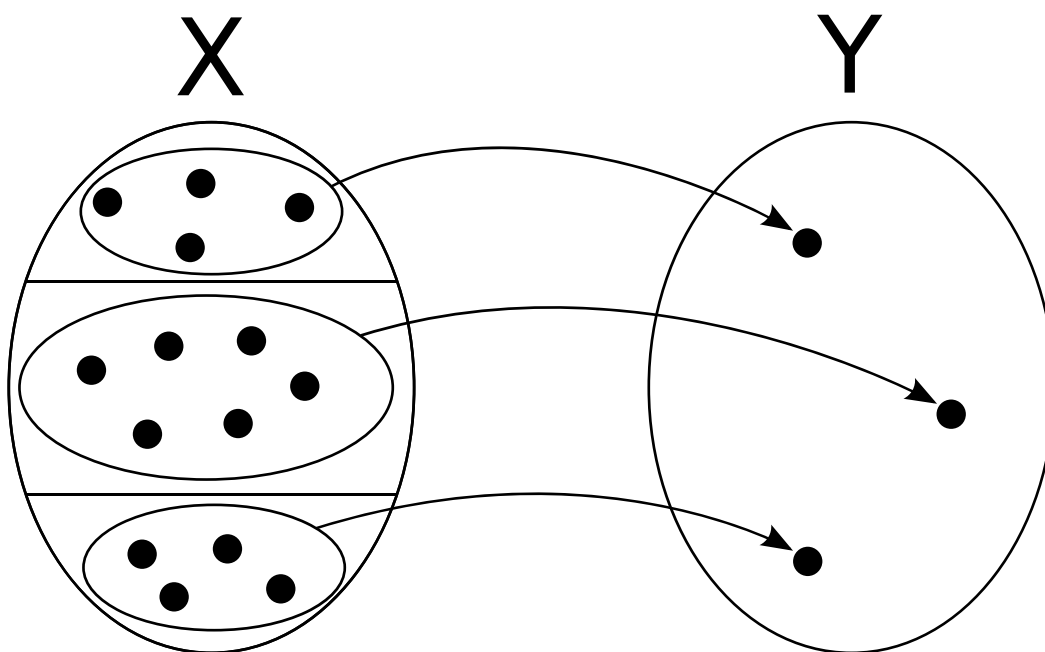
Sats: Antalet surjektioner



är $k! \cdot S(n; k)$

Ty:

Varje partition i k delar motsvarar precis $k!$ surjektioner.



$$X_i = \{x \in X \mid f(x) = y_i\}$$

$k!$ bijektioner

$$\{X_i\} \rightarrow Y$$

Exempel:

På hur många sätt kan 8 gäster fördelas på 5 hotellrum om inget rum lämnas tomt?

Tydligen söks antalet surjektioner

$$\{\text{gäster}\} \rightarrow \{\text{hotellrum}\}$$

så:

$$5! \cdot S(8; 5) \text{ sätt}$$

$$S(8; 5) = S(7; 4) + 5 \cdot S(7; 5) = \{\text{se triangeln}\} = \\ = 350 + 5 \cdot 140 = 1050$$

Så antalet sätt:

$$120 \cdot 1050 = 126000$$

På hur många sätt går det om H och D inte får dela?

Jo, alla fördelningar utom dem där del delar rum.

$$H \text{ och } D \text{ delar i } 5! \cdot S(7; 5) = 120 \cdot 140 = 16800 \text{ fall.}$$

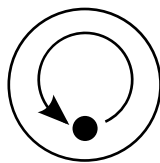
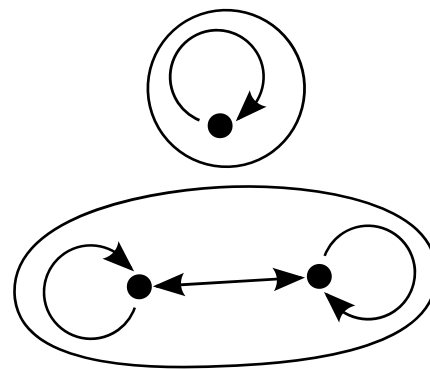
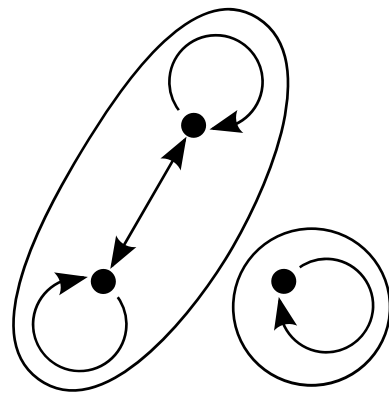
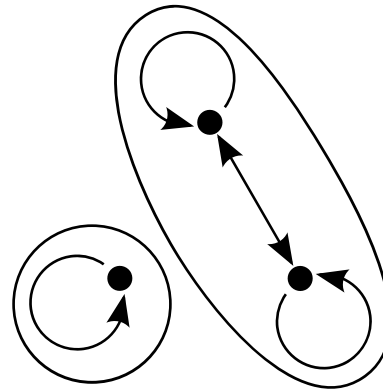
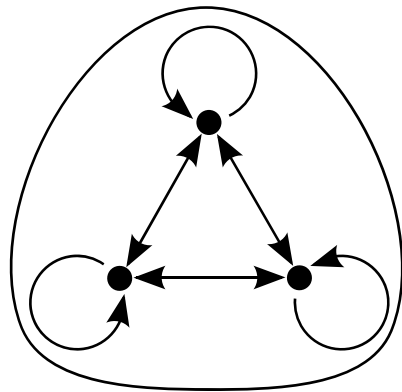
$$\text{Sökta antalet: } 126000 - 1600 = 105200$$

Varje partition i en mängd motsvarar precis en ekvivalensrelation på mängden. Så antalet ekvivalensrelationer är

$$\sum_{k=1}^n S(n; k) = n! \text{e radsummand i "Stirlings triangel".}$$

Exempel:

$n = 3$:



Exempel:

Varför gäller:

$$k^n = \sum_{i=1}^{\min(k; n)} S(n; i) (k)_i ?$$

Exempel:

$$n = 5, k = 3$$

$$\begin{aligned} HL &= S(5; 1)(3)_1 + S(5; 2)(3)_2 + S(5; 3)(3)_3 = \\ &= 1 \cdot 3 + 15 \cdot 3 \cdot 2 + 25 \cdot 3 \cdot 2 \cdot 1 = \\ &= 243 = 3^5 \end{aligned}$$

VL: Antalet funktioner

n-mängd \rightarrow k-mängd

$S(n; i)(k)_i$ antalet funktioner som tar precis i strycken värden.

2011-(02)feb-28: dag 5, 12

1)

n stycken likadana tärningar.
Hur många möjliga utfall?

(Vi antar att de har 6 sidor vardera.)

Oordnat urval med upprepning.

$$\binom{n + 6 - 1}{n} = \binom{n + 5}{n} = \binom{n + 5}{5}$$

2)

Antalet 5-siffriga tal (eventuellt med inledande 0:or).

a)

Totalt 10^5 stycken (ordnat urval med upprepning)

b)

Strikt växande, till exempel 02578.

$$\binom{10}{5} = 252 \text{ stycken}$$

c)

Växande inte strikt, till exempel 46889.

Ges biljekativt av hur många gånger varje siffra ingår.
Oordnat val med upprepning.

$$\binom{5 + 10 - 1}{5} = \binom{14}{5} = 2002 \text{ stycken}$$

d)

Ej strikt växande eller ej strikt avtagande (inklusive konstant)

$$2 \cdot \binom{14}{5} - 10 = 2 \cdot 2002 - 10 = 3994$$

... - 10 ty konstant ingår i både växande och avtagande.
($|A \cup B| = |A| + |B| - |A \cap B|$)

3)

Givet 12 strycken tvåsiffriga tal (bas 10).
Visa att två har skillnad aa_{10} ($a = 0, 1, \dots, 9$).

Av 12 tal är minst 2 stycken lika (mod 11), skillnaden 0 (mod 11).

Lösning:

$$a \cdot 11 \text{ något } a \quad \text{skillnaden: } 0 \leq aa \leq 99$$

4)

$$a_1, a_2, \dots, a_n \in \mathbb{Z}$$

Visa att någon icke-tom delmängd har summan delbar med n .

$$\text{Låt } s_i = a_1 + a_2 + \dots + a_i \quad i = 1, 2, \dots, n$$

Antingen är något s_i delbart med n (så klara) eller så är två av dem lika (mod n) (postfacksprincipen) och deras skillnad ($s_j - s_i = a_{i+1} + a_{i+2} + \dots + a_j$) delbar med n , också klart.

5)

Bokstäverna A, B, D, G, J och U kastas om.
På hur många sätt kan det ske utan att "DU" eller "JAG" ingår?

$$\text{Låt } A = \{\text{de som innehåller "DU"}\}$$

$$B = \{\text{de som innehåller "JAG"}\}$$

$$\mathcal{U} = \{\text{alla}\}$$

$$\begin{aligned} \text{Sökt } |\mathcal{U} \setminus (A \cup B)| &= |\mathcal{U}| - |A \cup B| = \\ &= |\mathcal{U}| - |A| - |B| + |A \cap B| = \\ &= 6! - 5! - 4! + 3! = \\ &= 720 - 120 - 24 + 6 = 582 \end{aligned}$$

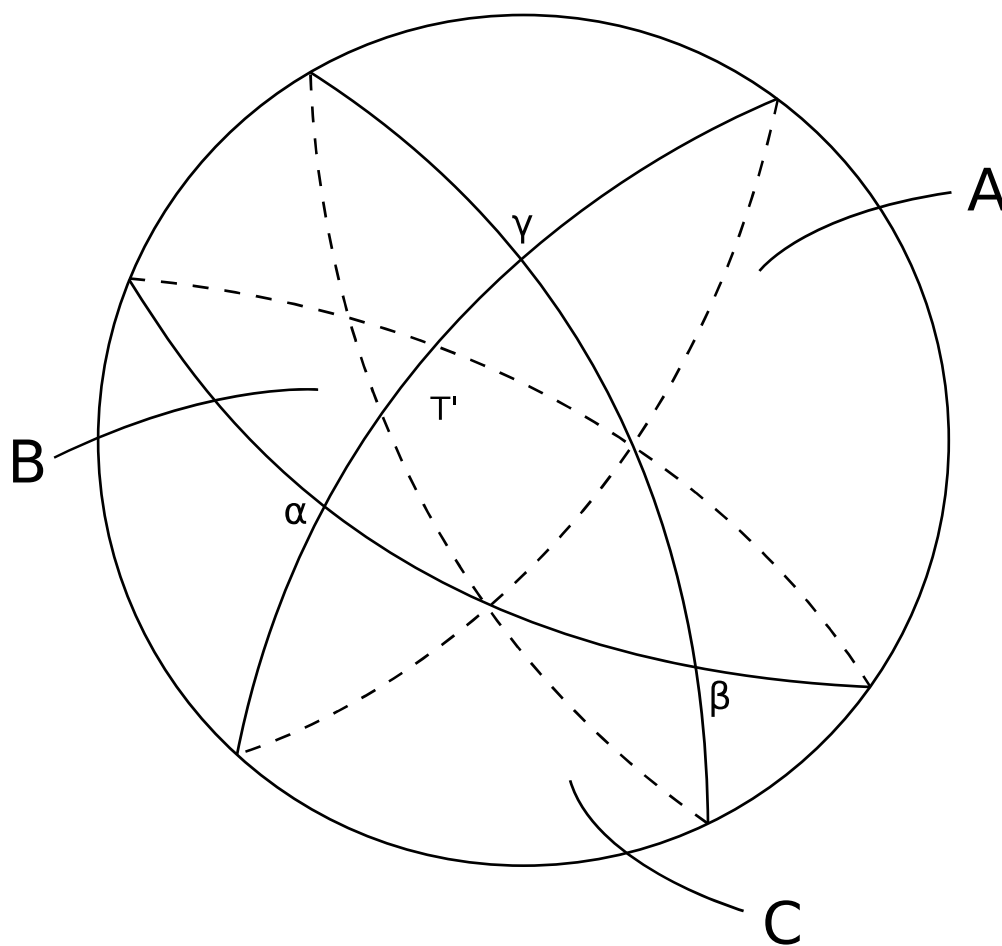
6)

En sfärisk triangel har vinklarna α , β och γ och sfären har radien R .
Vad är dess area?

Jo, inklusion och exklusion för areor

$$T = A \cap B \cap C$$

med A , B , C som halv-sfärer enligt figuren.



Triangeln T' ("mittemot" T) har samma area som T .

$$T' = S \setminus (A \cup B \cup C)$$

$$\begin{aligned}
|T| &= |T'| = |S \setminus (A \cup B \cup C)| = \\
&= |S| - |A \cup B \cup C| = \\
&= |S| - (|A| + |B| + |C|) + (|A \cap B| + |B \cap C| + |C \cap A|) - |A \cap B \cap C| = \\
&\quad \underbrace{4\pi R^2}_{\uparrow} \quad \underbrace{3 \cdot 2\pi R^2}_{\uparrow} \quad \underbrace{\frac{\gamma}{2\pi} 4\pi R^2}_{\uparrow} \quad \underbrace{\frac{\alpha}{2\pi} 4\pi R^2}_{\uparrow} \quad \underbrace{\frac{\beta}{2\pi} 4\pi R^2}_{\uparrow} \quad \underbrace{|T|}_{\uparrow} = \\
&= -2\pi R^2 + (\alpha + \beta + \gamma) \cdot 2R^2 - |T| \\
2 \cdot |T| &= -2\pi R^2 + (\alpha + \beta + \gamma) \cdot 2R^2 \\
2 \cdot |T| &= (\alpha + \beta + \gamma - \pi) \cdot 2R^2 \\
|T| &= (\alpha + \beta + \gamma - \pi) \cdot R^2
\end{aligned}$$

7)

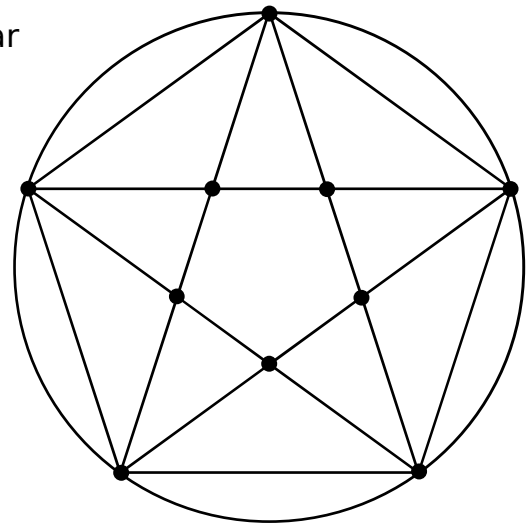
Hur många skärpunkter mellan diagonalerna (kordorna!) i cirkeln

Observera att skärningspunkterna motsvarar bijektivt mängder av fyra av punkterna på cirkeln.

$$\binom{5}{4} = \binom{5}{1} = 5$$

Så antalet skärningspunkter = antalet 4-delmängder till en n-mängd, det vill säga

$$\binom{n}{4}.$$



9)

Hur många fördelningar av 7 synder bland 4 personer är möjliga?

a)

Fördelningen kan beskrivas som en funktion

$$\{\text{synderna}\} \rightarrow \{\text{personerna}\}$$

(ingen synd hos mer än en person) och den funktionen är en surjektion.

(varje person har minst en synd).

Så sökt är antalet surjektioner från en 7-mängd till en 4-mängd.

$$4! \cdot S(7; 4) = 24 \cdot 350 = 8400$$

b)

Om ingen är girig och lat: dra port de fördelningarna.

$$4! \cdot S(6; 4) = 24 \cdot 65 = 1560$$

$$\text{Så svaret i b: } 8400 - 1560 = 6840$$

10)

På hur många sätt kan 7 kulor fördelas på 4 (särskiljbara) lådor i följande fall:

	kulor	tomma	svar:
a)	olika	ja	7-mängd \rightarrow 4-mängd $= 4^7 = 16384$
b)	olika	nej	Surjektion $(\cdot =7) \rightarrow (\cdot =4) = 4! \cdot S(7;4) = 8400$
c)	identiska	ja	Oordnat val med upprepning. $\binom{7+4-1}{4-1} = 120$
d)	identiska	nej	$\binom{3+4-1}{4-1} = 20$

Och för 4 icke-särskiljbara lådor, men 7 särskiljbara kulor:


tomma

e) ja $S(7; 1) + S(7; 2) + S(7; 3) + S(7; 4) = 715$

f) nej $S(7; 4) = 350$

Interlude...

Partitioner av heltal $n = n_1 + n_2 + \dots + n_k$, $n_1 \geq n_2 \geq \dots \geq n_k \geq 1$.
Antalet partitioner av n i k delar $P_k(n)$ ($\neq S(n; k)$).


identiska element särskiljbara element

Exempel:

Partitioner av $n = 5$

$[5], [4, 1], [3, 2], [3, 1^2], [2^2, 1], [2, 1^3], [1^5]$

$$P_1(5) = 1, P_2(5) = 2, P_3(5) = 2, P_4(5) = 1, P_5(5) = 1$$

... end of interlude.

(10) Och för icke-särskiljbara lådor och kulor:

tomma

g) ja $P_1(7) + P_2(7) + P_3(7) + P_4(7) = 1 + 3 + 4 + 3 = 11$

h) nej $P_4(7) = 3$

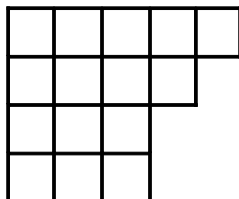
Exempel:

Låt $f_m(n)$ vara antalet partitioner av n i högst m delar,
och $g_m(n)$ vara antalet partitioner av m i delar $\leq n$.

Visa att $f_m(n) = g_m(n)$.

Varje partition svarar mot en tablå.

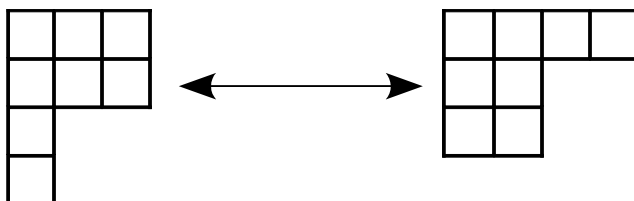
Till exempel $[5, 4, 3^2]$



$f_m(n)$ antalet tablåer med högst m rader.

$g_m(n)$ antalet tablåer med varje rad $\leq m$.

En bijektion mellan mängderna tablåer är
spegling i diagonalen (transponering):



Så lika många.

Modul 3

2011-(03)mar-02: dag 1, 13

Algebra

Grupper

Gruppdefinitionen
Ändliga grupper, grupptabeller

Abelska grupper

Ekvationslösning i grupper

Grupptabeller är en latinsk kvadrat

Ordning

Ordningen för en grupp, $|G|$

Ordningen för ett gruppelement, $o(g)$

Cyklisk grupper, $G = \langle g \rangle$

Generatorer, genererande element

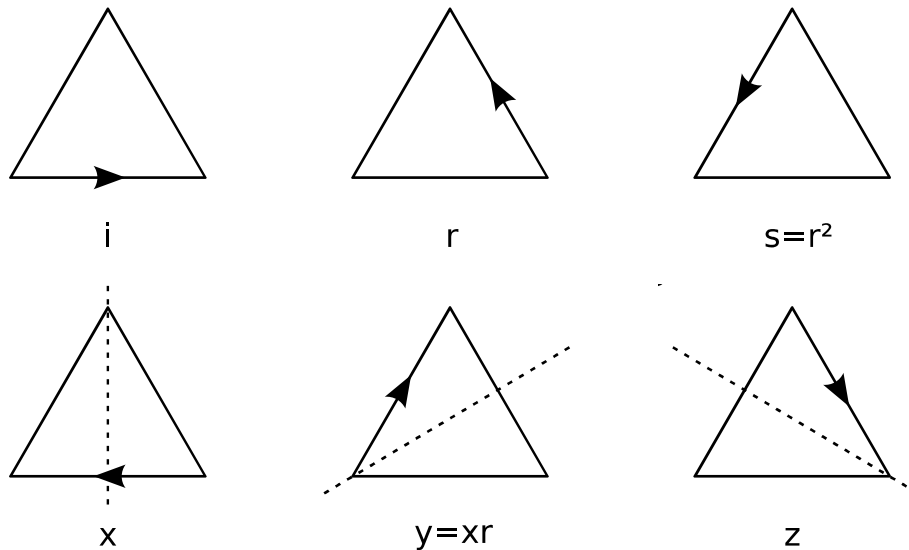
Övnings-KS 2

Vi börjar med “abstrakt algebra”, mest om grupper.

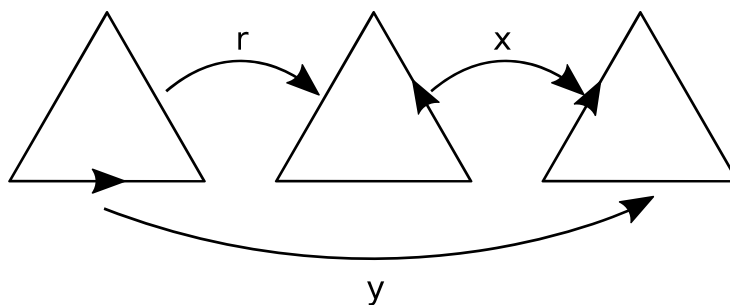
Exempel:

Symmetrier för en liksidig triangel
(det vill säga stela avbildningar som för över \triangle_i sig själv).

Alla symmetrier $G_{\triangle} = \{i, r, s, x, y, z\}$



$y = xr$ “först r , sedan x ”



$ix = xi = x$

Definition:

$(G; *)$ är en grupp om

G1) $x * y \in G \forall x, y \in G$
"slutenhet"

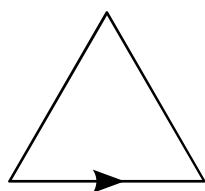
G2) $(x * y) * z = x * (y * z) \forall x, y, z \in G$
"associativitet"

G3) $\exists I \in G : I * x = x * I = x \forall x \in G$
"identitetselement"

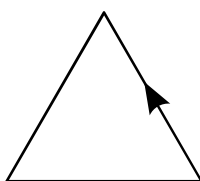
G4) $\forall x \in G \exists x^{-1} \in G : x * x^{-1} = x^{-1} * x = I$
"invers"

$(G_{\Delta}; \cdot)$ är en grupp ty axiomen G1, ..., G4 är uppfyllda.

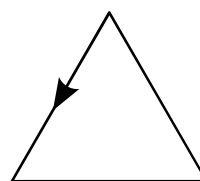
Symmetrigrupper för en liksidig triangel, G_{Δ}



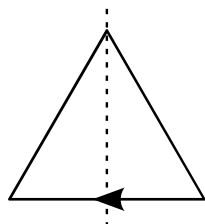
i



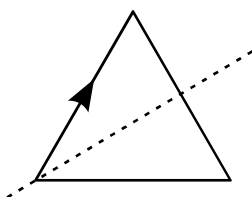
r



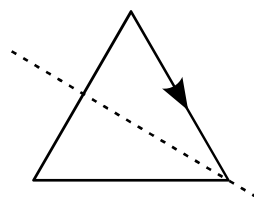
$s=r^2$



x



$y=xr$



$z=xr^2$

	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	z	x	y
s	s	i	r	y	z	x
x	x	y	z	i	r	s
y	y	z	x	s	i	r
z	z	x	y	r	s	i

	i	r	r ²	x	xr	xr ²
i	i	r	r ²	x	xr	xr ²
r	r	r ²	i	xr ²	x	xr
r ²	r ²	i	r	xr	xr ²	x
x	x	xr	xr ²	i	r	r ²
r	xr	xr ²	x	r ²	i	r
xr ²	xr ²	x	xr	r	r ²	i

$$r^3 = x^2 = i$$

$$rx = xr^2$$

Andra exempel på grupper:

Oändliga: $(\mathbb{Z}; +)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$, $(GL(n; \mathbb{R}); \cdot)$

reella $n \times n$ -matriser med $\det \neq 0$

Ändliga: G_Δ , S_n , $(\mathbb{Z}_m; +)$, $(\mathbb{Z}_p \setminus \{0\}; \cdot)$, $\left(\{x \in \mathbb{R} \mid -1 < x < 1\}, x * y = \frac{x + y}{xy + 1} \right)$

p , primtal

En grupps struktur bestäms helt av gruptabellen.

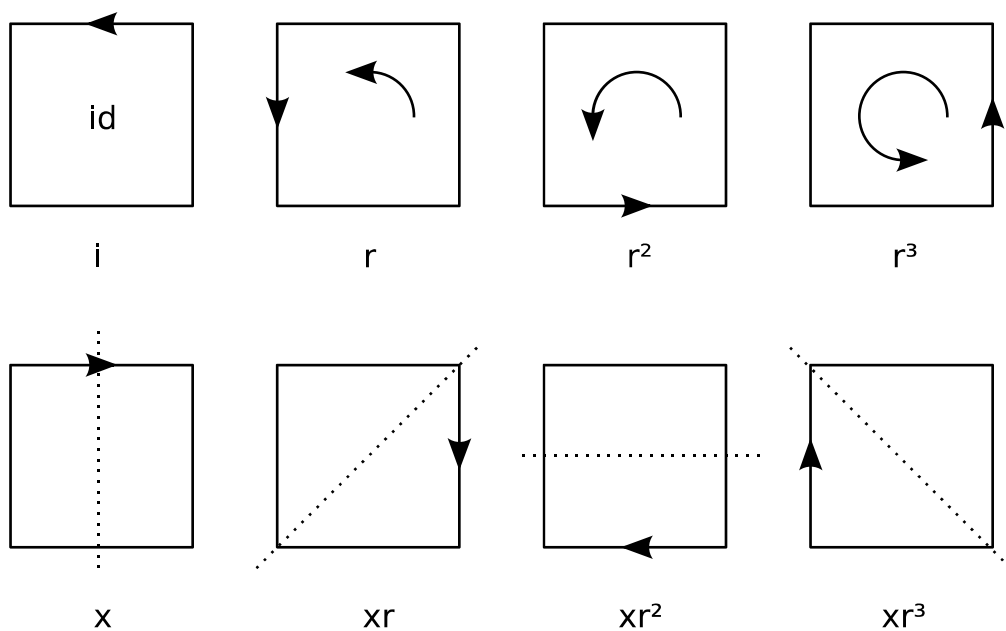
Exempel:

$(\mathbb{Z}_5; +)$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$1 = 0$ här. Inversen (under $+$) till 3: $-3 = 2$ ty $2+3 = 3+2 = 0$.

Symmetrigruppen för en kvadrat, G_{\square}



$$r^4 = x^2 = i$$

$$rx = xr^3$$

	i	r	r ²	r ³	x	xr	xr ²	xr ³
i	i	r	r ²	r ³	x	xr	xr ²	xr ³
r	r	r ²	r ³	i	xr ³	x	xr	xr ²
r ²	r ²	r ³	i	r	xr ²	xr ³	x	xr
r ³	r ³	i	r	r ²	xr	xr ²	xr ³	x
x	x	xr	xr ²	xr ³	i	r	r ²	r ³
xr	xr	xr ²	xr ³	x	r ³	i	r	r ²
xr ²	xr ²	xr ³	x	xr	r ²	r ³	i	r
xr ³	xr ³	x	xr	xr ²	r	r ²	r ³	i

Om det i en grupp $(G; *)$ gäller att

$$a * b = b * a$$

för alla $a, b \in G$, kallas G abelsk eller kommutativ.

Exempel:

Abelska:

$$(\mathbb{Z}_m; +), (\mathbb{R}_+; \cdot), (\mathbb{Z}_p \setminus \{0\}; \cdot), (\{e\}; *), (\mathbb{R}^n; +), (\mathbb{Z}; +)$$

Icke-abelska:

$$G_\Delta, G_\square, (GL(n; \mathbb{R}); \cdot) \quad n \geq 2$$

Exempel på allmän sats för grupper:

Om $a, b \in G$, G är grupp så har $ax = b$ och $ya = b$ entydig lösning, x, y .

Ty: Existens:

$x = a^{-1}b$ är en lösning:

$$ax = a(a^{-1}b) \stackrel{\overline{G_2}}{=} (aa^{-1})b \stackrel{\overline{G_4}}{=} 1b \stackrel{\overline{G_3}}{=} b$$

Entydighet:

Om x är en lösning:

$$\begin{aligned} ax = b &\Rightarrow a^{-1}(ax) = a^{-1}b \Rightarrow \{G2\} \Rightarrow (a^{-1}a)x = a^{-1}b \Rightarrow \{G4\} \Rightarrow \\ &\Rightarrow 1x = a^{-1}b \Rightarrow \{G3\} \Rightarrow x = a^{-1}b \end{aligned}$$

Andra ekvationen på samma sätt:

$$y = ba^{-1}$$

Så grupptabeller är latinska kvadrater.

*	x
a	(b)

Precis en gång i varje rad.
Även en gång i varje kolumn.

Satsen ger också att man alltid kan förkorta:

$$ax = ay \Rightarrow x = y \Leftarrow xa = ya$$

Exempel:

$G = \{e, a, b, c\}$ är en grupp (med \cdot) och $x^2 = e$ för alla $x \in G$.
4 olika

Finn dess grupptabell!

Identitetselement?

$$e^2 = e = e1 \Rightarrow e = 1$$

Identitetselement.

·	e	a	b	c	
e	e	a	b	c	← $x = e$
a	a	e	c	b	
b	b	c	e	a	Inte a, -e (rad) eller b (kolumn)
c	c	b	a	e	

\uparrow
 $ex = x$

\nwarrow
 $x^2 = e$

G är abelsk

Allmän sats:

Om $|G| = p^2$ (p , primtal) så är G abelsk.

Ordningen för en grupp G : $|G|$

Ordningen för ett element $g \in G$: $o(g)$,

det minsta > 0 sådant att $g^n = 1$ (1 identitetselement),
 ∞ om inget sådant finns.

Exempel:

$$|G_\Delta| = 6, \quad o(x) = 2, \quad o(r) = 3, \quad o(i) = 1$$

$$\begin{matrix} y & s \\ z & \in G_\Delta \\ \in G_\Delta \end{matrix}$$

Sats:

Om $g \in G$, en grupp, och $o(g) = m$, $g^s = 1$ (identitetselement) $\Leftrightarrow m|s$.

Ty:

\Rightarrow : Låt $g^s = 1$ och $s = qm+r$, $0 \leq r < m$.

$$\text{så } 1 = g^s = (g^m)^q \cdot g^r = 1^q \cdot g^r = g^r$$

så $r = 0$ enligt definitionen av $o(g)$.

\Leftarrow : Klart.

Definition:

En grupp, G , är cyklisk om det finns ett element $g \in G$ sådant att varje element i G är av formen g^n , något $n \in \mathbb{Z}$.

Ett sådant g kallas en generator, ett genererande element för G .

$$G = \langle g \rangle$$

Om $o(g) = m$:

$$G = \{1, g, g^2, g^3, \dots, g^{m-1}\} \text{ ser ut som } (\mathbb{Z}_m; +).$$

alla olika

Om $G = \langle g \rangle$ gäller $|G| = o(g)$

$o(g) = \infty$:

$$G = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\} \text{ ser ut som } (\mathbb{Z}; +).$$

Exempel:

$$(\mathbb{Z}_{12}; +) = \langle 5 \rangle \text{ ty}$$

n	0	1	2	3	4	5	6	7	8	9	10	11	(12)
ng	0	5	10	3	8	1	6	11	4	9	2	7	(0)

2011-(03)mar-09: dag 2, 14

Mer algebra

Delgrupper

Att känna igen dem.

$Z(G)$, $C(g)$

Sidoklasser

Lagranges sats

Grupper av primtalsordning är cykliska

Gruppisomorfi

“Strukturlikhet”

Från 2011-(03)mar-02, dag 13:

$(G; *)$ är en grupp om

G1) $x * y \in G \forall x, y \in G$
“slutenhet”

G2) $(x * y) * z = x * (y * z) \forall x, y, z \in G$
“associativitet”

G3) $\exists I \in G : I * x = x * I = x \forall x \in G$
“identitetsselement”

G4) $\forall x \in G \exists x^{-1} \in G : x * x^{-1} = x^{-1} * x = I$
“invers”

Idag om delgrupper

Definition:

Om $H \subseteq G$ och $(G; *)$ är en grupp så kallas H en delgrupp till G omm $(H; *)$ är en grupp.

Exempel:

$H = \{i, y\}$ är en delgrupp till G_{Δ} .

Ty:

G1 OK

G2 OK (ty, uppfyllt i G_{Δ})

G3 OK (i, identitetselement)

$$G4 \text{ OK } \begin{cases} i^{-1} = i \\ y^{-1} = y \end{cases}$$

Sats:

Om $H \subseteq G$ och $(G; *)$ är en grupp så är H en delgrupp till G omm:

$$\begin{cases} S0: & H \neq \emptyset \\ S1: & x, y \in H \Rightarrow x * y \in H \\ S2: & x \in H \Rightarrow x^{-1} \in H \end{cases}$$

Om H är ändlig räcker S0 och S1, ty:

\Rightarrow : klart

\Leftarrow : $S1 \Rightarrow G1$; $G2 \text{ i } G \Rightarrow G2 \text{ i } H$;

$x \in H \xrightarrow{S2} x^{-1} \in H$, så $\underbrace{xx^{-1}}_{S1} = 1 \in H$, så G3.

$S2 \Rightarrow G4$

Om H är ändlig, $H = \{h_1, h_2, \dots, h_n\}$ så om $x \in H \Rightarrow$

$\stackrel{S1}{\Rightarrow} x^2, x^3, \dots \in H$, så $x^k = x^l$ några $k > l \geq 0$ så

$$x^{k-l} = 1, \underbrace{x \cdot x^{k-l-1}}_{x^{-1}} = 1 = (xx^{-1}) \Rightarrow x^{-1} \in H, S2$$

Fler exempel på delgrupper till G :

$\{1\}$ och G är delgrupper till G

$\{i, r, s\}$ och $\{i, z\}$ delgrupper till G_Δ

$SL(n; \mathbb{R}) = \{\mathbf{A} \in GL(n; \mathbb{R}) \mid \det \mathbf{A} = 1\}$ delgrupp till $GL(m; \mathbb{R})$

$Z(G) = \{z \in G \mid zg = gz, \text{ alla } g \in G\}$, G 's centrum, en delgrupp till G :

S0 OK ($1 \in Z(G)$)

S1 OK ($x, y \in Z(G) \Rightarrow xyg = gxy$, alla $g \in G$ så $xy \in Z(G)$)

S2 OK:

$z \in Z(G) \Rightarrow zg = gz$, alla $g \in G \Rightarrow$

$$\Rightarrow \begin{cases} z^{-1}zg z^{-1} = gz^{-1} \\ z^{-1}zg z^{-1} = z^{-1}gzz^{-1} = z^{-1}g \end{cases} \quad \text{alla } g \in G$$

\Downarrow

$$z^{-1} \in Z(G)$$

Exempel:

$$Z(G_\square) = \{i, r^2\}, \quad Z(G_\Delta) = \{i\}$$

$$G \text{ abelsk} \Leftrightarrow Z(G) = G$$

$$C(g) = \{x \in G \mid xg = gx\} \text{ för alla } g \in G$$



“centralisatorn” till G

är en delgrupp till G .

Ty:

$$S0: 1 \in G$$

$$S1: xy \in C(g) \Rightarrow xyg = gxy \Rightarrow xy \in C(g)$$

$$S2: x \in C(g) \Rightarrow xg = gx \Rightarrow gx^{-1} = x^{-1}g \Rightarrow x^{-1} \in C(g)$$

Då

$$Z(G) = \bigcap_{g \in G} C(g), \quad g \in Z(G) \Rightarrow C(g) = G$$

Till exempel:

$$G_{\square}: C(i) = C(r^2) = G_{\square},$$

$$C(r) = C(r^3) = \{i, r, r^2, r^3\},$$

$$C(x) = \{i, r^2, x, xr^2\} = C(xr^2)$$

Varje $g \in G$ ($o(g) = m$) genererar en delgrupp $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ till G , en cyklisk delgrupp.

Exempel:

$$\begin{array}{ll} x \in G_{\Delta} & \text{genererar } \{i, x\} = \langle x \rangle \\ r \in G_{\Delta} & \text{genererar } \{i, r, s\} = \langle r \rangle \end{array}$$

$$\text{då } o(g) = |\langle g \rangle|$$

Sidoklasser (en. cosets)

Definition: Om H är en delgrupp till G , $g \in G$, så är $gH = \{gh \mid h \in H\}$ en vänstersidoklass till H (en. left coset) och $Hg = \{hg \mid h \in H\}$ en högersidoklass till H (en. right coset).

Exempel:

$$\begin{array}{ll} G_{\square}: & r\{i, x\} = \{r, xr^3\} \quad \text{vänstersidoklass} \\ & \{i, x\}r = \{r, xr\} \quad \text{högersidoklass} \end{array}$$

Sats:

Om H är en delgrupp till G så är g_1H och g_2H identiska eller disjunkta.

Ty: Låt $x \in g_1H \cap g_2H$, vi skall visa att $g_1H = g_2H$.

$$x = g_1h_1 = g_2h_2, \quad h_1, h_2 \in H \quad \text{så} \quad g_1 = g_2h_2h_1^{-1} \quad \text{och om}$$

$$y \in g_1H \Rightarrow y = g_1(h \in H) = g_2h_2h_1^{-1}h \quad (h \in H) \Rightarrow y \in g_2H$$

$$\left. \begin{array}{l} \text{så} \quad g_1H \subseteq g_2H \\ \text{på samma sätt} \quad g_2H \subseteq g_1H \end{array} \right\} \Rightarrow g_1H = g_2H$$

De ger en partition av G (ekvivalensrelationen $g_2^{-1}g_1 \in H$)

(Om H är ändlig är) dessutom $|H| = |gH| = |Hg|$

Ty: $f: H \rightarrow gH$, $f(h) = gh$ är en bijektion.
(surjektion enligt definitionen av gH , injektion: $gh_1 = gh_2 \Rightarrow h_1 = h_2$)

Så vänster- och högersidoklasser ger partitioner av G i lika stora mängder.

Exempel:

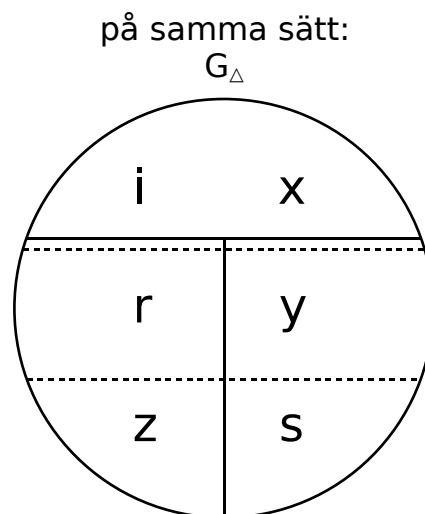
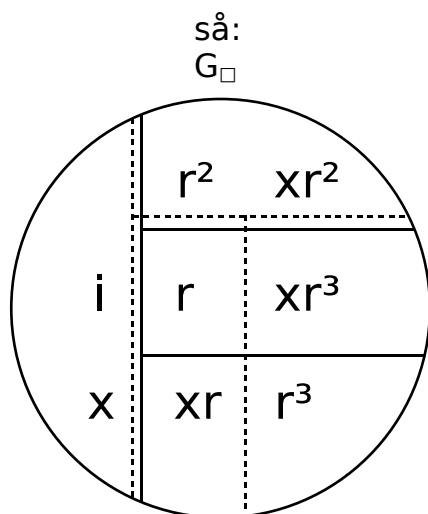
$$G_{\square}, \quad H = \{i, x\}:$$

Vänstersidoklasser:

$$\begin{aligned} iH &= \{i, x\} = xH \\ rH &= \{r, xr^3\} = xr^3H \\ r^2H &= \{r^2, xr^2\} = xr^2H \\ r^3H &= \{r^3, xr\} = xrH \end{aligned}$$

Högersidoklasser:

$$\begin{aligned} Hi &= \{i, x\} = Hx \\ Hr &= \{r, xr\} = Hxr \\ Hr^2 &= \{r^2, xr^2\} = Hxr^2 \\ Hr^3 &= \{r^3, xr^3\} = Hxr^3 \end{aligned}$$



Vänster- (heldraget) och höger- (halvdraget) -sidoklasser

$$\begin{aligned} \{i, x\}y &= \{y, r\} \\ y\{i, x\} &= \{y, s\} \end{aligned}$$

Så Lagranges sats: Om G är ändlig, H en delgrupp till G :

$$|H| \mid |G| \quad (\text{snyggare skrivit: } |H| \mid |G|, \text{ vilket jag kommer använda.})$$

(Definition:)

$$|G : H| = \frac{|G|}{|H|}, \quad H\text{:s index i } G, \text{ antalet (vänster eller höger) sidoklasser.}$$

Om $g \in G$, $o(g) = m$ så är $\langle g \rangle$ en delgrupp av ordning m .

Så sats:

Om G är en ändlig grupp och $g \in G$ så $o(g) \mid |G|$ och $g^{|G|} = 1$.

Exempel:

G_{Δ} har element av ordningarna 1, 2 och 3	$ G_{\Delta} = 6$
G_{\square} har element av ordningarna 1, 2 och 4	$ G_{\square} = 8$

Sats:

Om G är en grupp, $|G| = p$, p primtal så är G cyklisk.

Ty:

$$x \in G, x \neq 1, o(x) > 1, o(x) \mid p \Rightarrow o(x) = p$$

Alla element utom 1 är generatorer för G .

Definition:

En gruppisomorfi mellan $(G_1; *)$ och $(G_2; \circ)$ är en bijektion $\phi : G_1 \rightarrow G_2$ så att $\phi(g * g') = \phi(g) \circ \phi(g')$ för alla $g, g' \in G_1$.

Grupperna $(G_1; *)$, $(G_2; \circ)$ kallas isomorfa om det finns en isomorfi mellan dem.

$(G_1; *) \approx (G_2; \circ)$ (Beteckningen $(G_1; *) \cong (G_2; \circ)$ är mycket vanligare.)

Isomorfi är en ekvivalensrelation mellan grupper.

Exempel:

$$(\mathbb{R}; +) \cong (\mathbb{R}_+; \cdot) \quad (\approx)$$

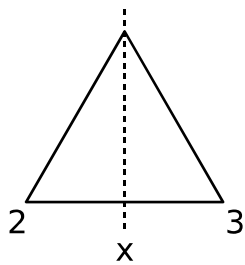
En isomorfi $\phi(x) = e^x$, ty ϕ är en bijektion och

$$\phi(x + y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$$

Exempel:

$G_{\Delta} \cong S_3$ -gruppen av bijektioner $\{1, 2, 3\} \rightarrow \{1, 2, 3\}$.

Isomorfin ges av avbildningen av triangelns hörn.



$$\phi(x): \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{cases}$$

(Kan även skrivas:)

$$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Exempel:

$$(\mathbb{Z}_5 \setminus \{0\}; \cdot) \cong (\mathbb{Z}_4; +)$$

2011-(03)mar-10: dag 3, 15

1) Vilket är identitetselementet?

Jo, $a * c = c$ ger a är identitetselement \rightarrow ger rad 1 och kolumn 1.

Grupptabellen är en latinsk kvadrat, så $c * f = b$, ...

*	a	b	c	d	f	g
a	a	b	c	d	f	g
b	b	a	g	f	d	c
c	c	f	a	g	b	a
d	d	g	f	a	c	b
f	f	c	d	b	g	a
g	g	d	b	c	a	f

a) Gruppen är inte abelsk, ty $b * c = g \neq f = c * b$.

b) $a * c = 1 * c$ ger $a = 1$ som ovan.

c) Inverser: $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$, $d^{-1} = d$, $f^{-1} = g$, $g^{-1} = f$

ty till exempel $f * g = a (= 1)$

d) $o(a) = 1$, $o(b) = o(c) = o(d) = 2$, $o(f) = o(g) = 3$

ty $b^2 = a$, men $b^{-1} \neq a$, $f^1 \neq a$, $f^2 = g \neq a$, $f^3 = a$.

Cykliska delgrupper:

$$\langle a \rangle = \{a\}$$

$$\langle b \rangle = \{a, b\}$$

$$\langle c \rangle = \{a, c\}$$

$$\langle d \rangle = \{a, d\}$$

$$\langle f \rangle = \{a, f, g\}$$

$$\langle g \rangle = \{a, g, f\}$$

$$\langle f \rangle = \{a, f, g\} = \langle g \rangle$$

e) $\underline{a * b * c * d * f * g} = b * g * a = c * a = c$

2) G en grupp med identitetselement 1, $a, b, c, d \in G$

a) Finn det $x \in G$ som uppfyller (givet att ett sådant finns)

$$\begin{cases} ax^2 = b \\ x^3 = 1 \end{cases}$$

$$ax^2 = b \Rightarrow ax^3 = bx \Rightarrow \{x^3 = 1\} \Rightarrow a = bx \Rightarrow x = b^{-1}a$$

b) På samma sätt

$$\begin{cases} (xax)^3 = bx & (1) \\ x^2a = (xa)^{-1} & (2) \end{cases}$$

$$bx = \{(1)\} = (xax)^3 = xax^2ax^2ax = \{(2)\} = \\ = xa(xa)^{-1}(xa)^{-1}x = (xa)^{-1}x$$

$$\text{så } bxa = (xa)^{-1}xa = 1$$

$$\text{så } x = b^{-1}a^{-1}$$

d) Visa $(abc)^{-1} = abc \Rightarrow (bca)^{-1} = bca$

$$\text{Jo, } (abc)^{-1} = abc \Rightarrow \underline{bca \cdot bca} = bc(abc)^{-1}a = \\ = \underline{a^{-1}abc(abc)^{-1}a} = a^{-1} \cdot 1 \cdot a = 1$$

$$\text{så } bca = (bca)^{-1}$$

$$bca \cdot bca = 1 = bca \cdot (bca)^{-1}$$

f) Visa $b^2ab = a^{-1} \Rightarrow$ det finns $s \in H$ med $a = s^3$

$$\text{Jo, } b^2ab = a^{-1} \Rightarrow ba = b^{-1}a^{-1}b^{-1}$$

$$\underline{(ba)^3} = b^{-1}a^{-1}\underline{b^{-1} \cdot b}aba = b^{-1}\underline{a^{-1}a}ba = \underline{b^{-1}ba} = \underline{a}$$

3) $G_1 = (\mathbb{Z}_8; +)$, $G_2 = (U(\mathbb{Z}_{15}); \cdot)$

De invertibla elementen i \mathbb{Z}_{15} ,
det vill säga alla x med $\text{sgd}(x; 15) = 1$

a) Grupptabeller:

$G_1:$	+	0	1	2	3	4	5	6	7
0		0	1	2	3	4	5	6	7
1		1	2	3	4	5	6	7	0
2		2	3	4	5	6	7	0	1
3		3	4	5	6	7	0	1	2
4		4	5	6	7	0	1	2	3
5		5	6	7	0	1	2	3	4
6		6	7	0	1	2	3	4	5
7		7	0	1	2	3	4	5	6

$G_2:$	\cdot	1	2	4	7	8	11	13	14
1		1	2	4	7	8	11	13	14
2		2	4	8	14	1	7	11	13
4		4	8	1	13	2	14	7	11
7		7	14	13	4	11	2	1	8
8		8	1	2	11	4	13	14	7
11		11	7	14	2	13	1	8	4
13		13	11	7	1	14	8	4	2
14		14	13	11	8	7	4	2	1

$(U(\mathbb{Z}_m); \cdot)$ är en grupp för alla $m = 1, 2, \dots$

$$G1) \quad \forall x, y \in G : x * y \in G$$

$$G2) \quad \forall x, y, z \in G : (x * y) * z = x * (y * z)$$

$$G3) \quad \exists 1 \in G : \forall x \in G : 1 * x = x * 1 = x$$

$$G4) \quad \forall x \in G : \exists x^{-1} \in G : x * x^{-1} = x^{-1} * x = 1$$

Ty:

$$G1: \quad x, y \in U(\mathbb{Z}_m) \Rightarrow (xy)^{-1} = x^{-1}y^{-1}$$

$$(xyy^{-1}x^{-1} = xx^{-1} = 1)$$

$$G2: \quad \cdot \text{ associativ i } \mathbb{Z}_m$$

$$G3: \quad 1 \in U(\mathbb{Z}_m), \text{ identitetselementet}$$

$$G4: \quad x \text{ invertabel ger} \\ (x^{-1})^{-1} = x \text{ så} \\ x^{-1} \text{ invertabel.}$$

b) Ordningar för elementen:

$o(x):$	1	2	4	8
$x \in G_1:$	0	4	2, 6	1, 3, 5, 7
$x \in G_2:$	1	4, 11, 14	2, 7, 8, 13	

- c) Cykliska delgrupper med sidoklasser
(vänster- = högersidoklass ty abelska grupper)

	Genererande element	delgrupper	sidoklasser
G_1 :	0	$\{0\}$	$\{0\}, \{1\}, \{2\}, \dots, \{7\}$
	4	$\{0, 4\}$	$\{0, 4\}, \{1, 5\}, \{2, 6\}, \{3, 7\}$
	2, 6	$\{0, 2, 4, 6\}$	$\{0, 2, 4, 6\}, \{1, 3, 5, 7\}$
	1	G_1	G_1

Alla singleton-delmängder i G_2

G_2 :	1	$\{1\}$	$\{g\}, g \in G_2$
	4	$\{1, 4\}$	$\{1, 4\}, \{2, 8\}, \{7, 13\}, \{1, 14\}$
	11	$\{1, 11\}$	$\{1, 11\}, \{2, 7\}, \dots$
	14	$\{1, 14\}$	$\{1, 14\}, \{2, 13\}, \dots$
	2, 8	$\{1, 2, 4, 8\}$	$\{1, 2, 4, 8\}, \{7, 14, 13, 11\}$
	7, 13	$\{1, 7, 4, 13\}$	$\{1, 7, 9, 13\}, \{2, 14, 8, 11\}$

- d) Alla delgrupper till G_2 ?

Del de cykliska enligt ovan, dels:
Ordningen måste vara 1, 2, 4 eller 8 (ty $|H| \mid 8$)

bara de cykliska

Ordning 4? Elementens ordning måste vara 1 eller 2.
(Ordningen 4 ger en cyklisk delgrupp!)
Ingen i G_1 (ty bara 0, 4 av ordningen 1, 2)
i G_2 kanske $\{1, 4, 11, 14\}$.

Sidoklasser:
 $\{1, 4, 11, 14\}, \{2, 7, 8, 13\}$

Ordning 8:

G_1 är cyklisk; $G_1 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.
 G_2 inte, inget element av ordning 8.

4) Är $G_1 = (U(\mathbb{Z}_8); \cdot)$, $G_2 = (U(\mathbb{Z}_{14}); \cdot)$ cykliska?

G är cyklisk om $o(g) = |G|$, för något $g \in G$.

$$G_1 = U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$$

$$G_2 = U(\mathbb{Z}_{14}) = \{1, 3, 5, 9, 11, 13\}$$

Ordningen för elementen:

G_1 :	g^1	g^2	g^3	g^4	ordning för g
	<u>1</u>				1
	3	<u>1</u>			2
	5	<u>1</u>			2
	7	<u>1</u>			2



Ingen 4 ($= |G_1|$) så G_1 är inte cyklisk.

G_2 :	g^1	g^2	g^3	g^4	g^5	g^6	ordning
	<u>1</u>						1
	3	9	13	11	5	<u>1</u>	6
	5	11	13	9	3	<u>1</u>	6
	9	11	<u>1</u>				3
	11	9	<u>1</u>				3
	13	<u>1</u>					2

Så G_2 är cyklisk.

$$G_2 = \langle 3 \rangle = \langle 5 \rangle$$

5) $G = (\mathbb{Z}_{13} \setminus \{0\}; \cdot)$ ($= (U(\mathbb{Z}_{13}); \cdot)$) är cyklisk. Finn alla generatorer.

$|G| = 12$ så vi söker $g \in G$ med $o(g) = 12$.

Möjliga ordningar: 1, 2, 3, 4, 6, 12, så
 $o(g) = 12$ om $g^4, g^6 \neq 1$.

g	1	2	3	4	5	6	7	8	9	10	11	12
g^4	1	3	3	4	1	9	9	1	9	3	3	1
g^6		<u>12</u>	1	1		<u>12</u>	<u>12</u>		1	1	<u>12</u>	
o		↑	↑			↑	↑				↑	
		$o(2) = 12$	$o(3) \neq 12$									

Generatorer: 2, 5, 7, 11

Potenser av 2

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	
2	4	8	3	6	12	11	9	5	10	7	1
6	10	...									

$$3 \cdot 11 = 2^4 \cdot 2^p = 2^{11}$$

logaritmer i bas 2.

6) Visa att $g^{32} = 1$ för alla $g \in U(\mathbb{Z}_{64}) = G$.

$$\begin{aligned} \text{Jo, } |U(\mathbb{Z}_{64})| &= |\{x \in \{0, 1, \dots, 63\} : \text{sgd}(x; 64) = 1\}| = \\ &= |\{1, 3, 5, \dots, 63\}| = 32 \end{aligned}$$

$$g^{|G|} = 1 \text{ alla } g \in G$$

2011-(03)mar-21: dag 4, 16

Mer algebra

Direkta produkter av grupper

Normala grupper

Ringar och kroppar

Permutationsgrupper

Direkta produkter av grupper

Från förra övningen

- 7) Definiera den direkta produkten $(G_1, *_1) \times (G_2, *_2) = (G_1 \times G_2, \circ)$ av $(g_1, g_2) \circ (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$.
 $g_1, h_1 \in G_1; g_2, h_2 \in G_2$

- a) Verifiera att detta är en grupp.

G1, Sluten:

Gäller eftersom det gäller för G_1 och G_2 .

$$\begin{aligned} g_1 *_1 h_1 &\in G_1 \\ g_2 *_2 h_2 &\in G_2 \end{aligned}$$

G2, Associativ:

Gäller eftersom det gäller för G_1 och G_2 .

$$\begin{aligned} \text{Vänsterelementet: } g_1 *_1 h_1 &\in G_1 \\ \text{Högerelementet: } g_2 *_2 h_2 &\in G_2 \end{aligned}$$

G3, Identitetsselement:

$$1 = (1_1, 1_2)$$

$$\begin{aligned} 1_1 &\text{ är identitetsselementet i } G_1. \\ 1_2 &\text{ är identitetsselementet i } G_2. \end{aligned}$$

$$(g_1, g_2) \circ (1_1, 1_2) = (g_1 *_1 1_1, g_2 *_2 1_2) = (g_1, g_2)$$

G4, Inverser:

$$(g, h)^{-1} = (g^{-1}, h^{-1})$$

$$(g, h) \circ (g^{-1}, h^{-1}) = (g *_1 g^{-1}, h *_2 h^{-1}) = (1_1, 1_2) = 1$$

$$(\mathbb{R}, +) \times (\mathbb{R}, +) = (\mathbb{R}^2, +)$$

- b) Visa att $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +) \cong (\mathbb{Z}_6, +)$
(Vi ska alltså visa isomorfi.)

Båda grupperna $[\mathbb{Z}_2 \times \mathbb{Z}_3$ och $\mathbb{Z}_6]$ är cykliska av ordningen 6.

En isomorfi:

$\mathbb{Z}_2 \quad \mathbb{Z}_3 \quad \mathbb{Z}_6$

$$\phi(0, 0) = 0$$

$$\phi(1, 1) = 1$$

$$\phi(0, 2) = 2$$

$$\phi(1, 0) = 3$$

$$\phi(0, 1) = 4$$

$$\phi(1, 2) = 5$$

$$\phi(0, 0) = 0$$

Detta är en isomorfi på grund av att båda är cykliska. Beror på additionen.

Däremot $(\mathbb{Z}_3, +) \times (\mathbb{Z}_3, +) \not\cong (\mathbb{Z}_9, +)$ eftersom alla element har ordning 1 eller 3 i \mathbb{Z}_3 , $(\mathbb{Z}_3, +) \times (\mathbb{Z}_3, +)$ är alltså inte cyklisk; det är dock \mathbb{Z}_9 .

Normala delgrupper

Definition: En delgrupp, N , till en grupp, G , är en normal delgrupp ($N \trianglelefteq G$) om vänstersidoklasser = högersidoklasser.

Det vill säga:

$$gN = Ng \quad \forall g \in G$$

Exempel: Alla delgrupper för abelska (kommutativa) grupper.

För G_{\square} : $\{i, r^2\}, \{i, r, r^2, r^3\}$

Om N är en normal delgrupp så bildas

$G/N = \{gN \mid g \in G\} = \{\text{normal}\} = \{Ng \mid g \in G\}$, kvotgruppen som är en grupp.

Motivieringen till namnet är: $|G| = |G/N| \cdot |N|$

$$g_1N \cdot g_2N = \{g_1n_1g_2n_2 \mid n_1, n_2 \in N\} = \{\text{normal}\} = \{g_1g_2n_3n_2 \mid n_3, n_2 \in N\} = g_1g_2N \quad \text{och} \quad g_1g_2N \leq g_1Ng_2N \quad \text{så} \quad g_1Ng_2N = g_1g_2N.$$

G/N med operationen $g_1Ng_2N = g_1g_2N$ är en grupp:

G1, Sluten: $g_1g_2N \in G/N \Rightarrow \{g_1g_2 = h\} \Rightarrow hN \in G/N$

G2, Associativ: $(g_1Ng_2N)g_3N = (g_1g_2)g_3N = g_1(g_2g_3)N = g_1N(g_2Ng_3N)$

G3, Identitetselement: $N = 1N$

G4, Inverser: $gN)^{-1} = g^{-1}N$

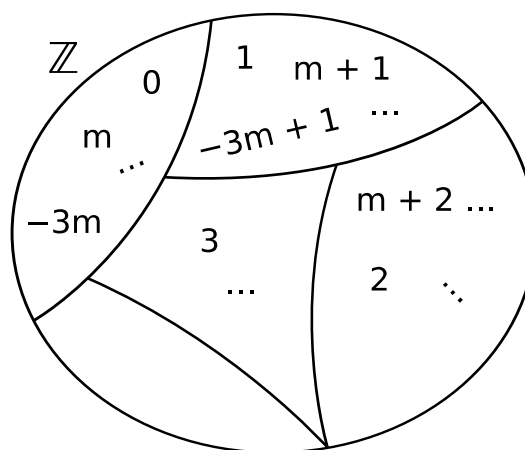
Exempel: $(\mathbb{Z}, +)$ (abelsk, så sidoklasserna är normala)

$(\mathbb{Z}, +) / (m\mathbb{Z}, +) = (\mathbb{Z}_m, +)$

G grupp

N normal delgrupp

$G/N = \{gN \mid g \in G\}$



Exempel: $N = \{i, r^2\}$

$G/N = \{\{i, r^2\} = e, \{r, r^3\} = a, \{x, xr^2\} = b, \{xr, xr^3\} = c\}$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$N = iN = r^2N$

$N = Ni = Nr^2$

$xN = Nx = xr^2N =$

$= Nxr^2$

Till exempel:

$$\begin{aligned}
 ab &= \{r, r^3\}\{x, xr^2\} = \\
 &= \{rx, rxr^2, r^3x, r^3xr^2\} = \\
 &= \{xr^3, xr^2r^3, r^3x, r^3xr^2\} = \\
 &= \{xr^3, xr, xr, xr^2r\} = \\
 &= \{xr^3, xr\}
 \end{aligned}$$

Gruppisomorfi: $\psi : G_1 \rightarrow G_2$ $((G_1, *), (G_2, \circ))$
 sådan att
 $\psi(g * h) = \psi(g) \circ \psi(h)$

Då är $G \cong G/N$
 Varje homomorfi ges så (av någon normal delgrupp)

Ringar är mängder med 2 operationer.

En ring $(R, \text{ med addition och multiplikation})$ betecknas $(R, +, \cdot)$,
 och definieras av: (Ringar liknar \mathbb{Z} .)

- (1) $(R, +)$ är en abelsk grupp, med identitetselement 0.
- (2) (R, \cdot) är sluten, associativ, med identitetselement 1.
- (3) Multiplikation (\cdot) är distributiv över addition $(+)$:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) = ab + ac \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c) = ac + bc \end{aligned}$$

Exempel på ringar:

$$\mathbb{Z}, \mathbb{Z}_m, M_n(\mathbb{R}), \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{R}[x]$$

$M_n(\mathbb{R})$ = $n \times n$ -matriser med element i ringen \mathbb{R} .

$\mathbb{R}[x]$ = Polynom med koefficienter i \mathbb{R} . (Polynom över \mathbb{R})

$(F, +, \cdot)$ (F skrivs ofta \mathbb{F}) är en kropp (en. field) om det är en ring sådan att
 $(F \setminus \{0\}, \cdot)$ är en abelsk grupp.

Exempel (p primtal):

$$\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p, F(x) = \left\{ \frac{p(x)}{q(x)} \mid \begin{array}{l} p, q \in F[x] \\ q(x) \neq 0 \end{array} \right\}$$

I en ring R : $x \in R$ kallas invertibel i R om det finns $u \in R$ sådant att
 $ux = xu = 1$; då är $u = x^{-1}$

$$U(R) = \{x \in R : x \text{ invertibelt}\}$$

Sats: $(U(R), \cdot)$ är en grupp för varje ring R .

Exempel: $U(\mathbb{Z}) = \{-1, 1\}$
 $U(\mathbb{Z}_m) = \{x \in \mathbb{Z}_m : \text{sgd}(x, m) = 1\}$

En permutation är en bijektiv funktion med samma domän som kodomän
(från en mängd till sig själv):

$$\pi : X \rightarrow X, \pi \text{ bijektiv}$$

S_n = mängden av alla permutationer av $[n] = \{1, 2, 3, \dots, n\}$

$$|S_n| = n! \quad (\text{Antalet permutationer})$$

(S_n, \circ) är en grupp:

- G1: En sammansättning av bijektioner är också en bijektion.
- G2: Associativitet gäller alltid för sammansättning av funktioner.
- G3: Identietspermutationen $\text{id}(x) = x$ är identiitselement.

$$\{1, 2, 3, \dots\} \rightarrow \{1, 2, 3, \dots\}$$

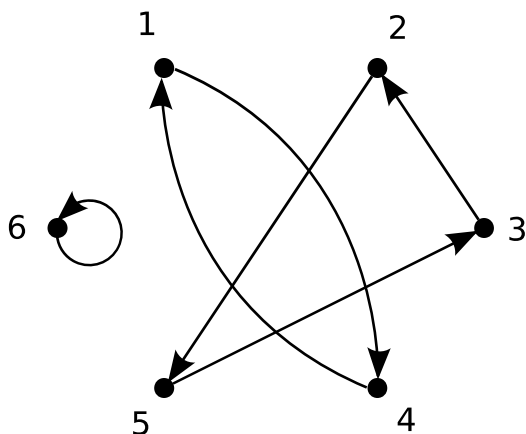
- G4: Inversen som funktion är inverselement.
Inversen av en bijektion är en bijektion.

Varje $g \in G$ (G grupp) ger en permutation av g .

$$\pi_g(h) = gh \quad \pi_g \in S_G \quad (G \text{ är isomorf med en delgrupp av } S_G)$$

För att beskriva permutationer

Till exempel $\pi \in S_6$:



Tvåradnotation som beskriver bijektionen:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}$$

Enradnotation:

$$[4 \ 5 \ 2 \ 1 \ 3 \ 6]$$

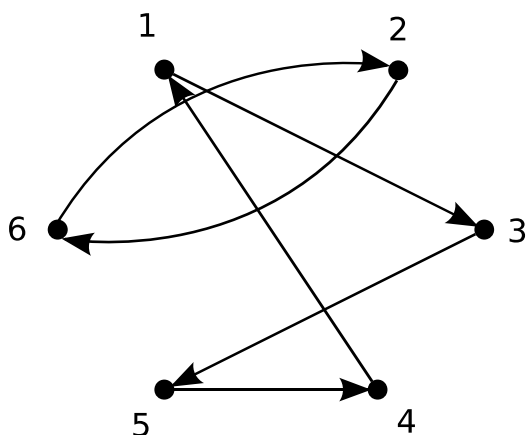
Det vill säga nedra raden i tvåradnotation och övre raden är underförstådd.

Cykelnotation:

$$(1 \ 4 \ 2)(2 \ 5 \ 3 \ 1)(6 \ 6) \\ \text{alltså:} \\ (1 \ 4)(2 \ 5 \ 3)(6)$$

Cykelnotation, börja någonstans och följ "avbildningspilarna" till man kommer tillbaka. Upprepa tills alla element har tagits med.

$\sigma \in S_6$



Tvåradnotation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 4 & 2 \end{pmatrix}$$

Enradnotation:

$$[3 \ 6 \ 5 \ 1 \ 4 \ 2]$$

Cykelnotation:

$$(1 \ 3 \ 5 \ 4)(2 \ 6)$$

Produkten i S_6 : (först σ sedan π)

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 4 & 2 \\ 2 & 6 & 3 & 4 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 4 & 1 & 5 \end{pmatrix} = (1 \ 2 \ 6 \ 5)(3)(4)$$

(id $\rightarrow \sigma$ i först-andra raden, $\sigma \rightarrow \pi$ i andra-tredje raden)

2011-(03)mar-24: dag 5, 17

Mer om permutationer

Produkter, inverser

Permutationsmatriser

Cayleys sats

Permutationers ordning

mgm av cykellängderna

Konjugering

En ekvivalensrelation på S_n

Permutationers typ (cykelstruktur)

Permutations paritet

Transpositioner

$$\operatorname{sgn} \pi = (-1)^{\alpha_2 + \alpha_4 + \dots} = (-1)^{n - c(\pi)}$$

Hälften jämna, hälften udda i S_n , $n \geq 2$

Determinanter

Mer om permutationer idag.

Exempeln från sist $\pi, \sigma \in S_b$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}$$

Cykelnotation: $(1\ 4)(2\ 5\ 3)(6)$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 4 & 2 \end{pmatrix}$$

Inte nödvändig, bara ett element.

Cykelnotation: $(1\ 3\ 5\ 4)(2\ 6)$

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 4 & 2 \\ 2 & 6 & 3 & 4 & 1 & 5 \end{pmatrix} \sigma \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 4 & 1 & 5 \end{pmatrix}$$

Skrivs inte

Oftare (produkt av cykelnotation = cykel):

$$\pi\sigma = \underbrace{(1\ 4)(2\ 5\ 3)}_{\text{cykel}} \underbrace{(1\ 3\ 5\ 4)(2\ 6)}_{\text{cykel}} = (1\ 2\ 6\ 5)(3)(4)$$

$$\sigma\pi = \underbrace{(1\ 3\ 5\ 4)(2\ 6)}_{\text{cykel}} \underbrace{(1\ 4)(2\ 5\ 3)}_{\text{cykel}} = (1)(2\ 4\ 3\ 6)(5)$$

$$\text{och } \pi^{-1} = (1\ 4)(2\ 3\ 5)(6)$$

Skurkarna (texten saknas):

Låt $X = \{\text{ä, v, u, t, m}\}$ vara de åtalade. Permutationerna $\pi : X \rightarrow X$ ges av att $\pi(i) = j$ betyder att personen i åtalas för brott som person j "heter".

(En permutation (bijektion) enligt förutsättningen: var och en namne till en annans brott)

så surjektiv, där med injektiv.

$\pi(i) \neq i \forall i \in X$ (enligt text)

Så π har inga 1-cykler, det vill säga kan vara $[5]$, $[2\ 3]$ (men inte $[1\ 4]$).

$\pi(\pi(\pi(n))) = m, \quad \pi(\pi(\pi(m))) = v,$ så n, m, v i samma cykel, inte en 3-cykel
 ty $\pi^3(n) \neq n$, så π har en 5-cykel:
 $(n \dots m \dots),$ så $(n \ v \dots m \dots)$ så $(n \ v \textcircled{a} m \ t)$
 $\therefore \pi(t) \neq m$ (enligt sista stycket)

Ett sätt till att beskriva permutationer:

$\pi \in S_n$ motsvarar \mathbf{M}_π med $m_{ij} = \begin{cases} 1 & \text{om } \pi(j) = i \\ 0 & \text{annars} \end{cases}$.

$$\mathbf{M}_\pi = \begin{pmatrix} 0 & 0 \\ 0 & \vdots \\ \vdots & 0 \\ 0 & \dots & 1 \\ 1 & 0 \\ 0 & \vdots \\ \vdots & \\ 0 & \end{pmatrix}$$

kolonn j
 rad $\pi(j)$
 rad $\pi(1)$

så $\mathbf{M}_\pi \mathbf{e}_j = \mathbf{e}_{\pi(j)}$ där $\mathbf{e}_k =$

$$= \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

rad k

Och $\underbrace{\mathbf{M}_\pi \mathbf{M}_\sigma}_{\substack{n \times n \\ n \times 1}} \mathbf{e}_j = \mathbf{M}_\pi \mathbf{e}_{\sigma(j)} = \mathbf{e}_{\pi(\sigma(j))} = \mathbf{e}_{(\pi\sigma)(j)} = \mathbf{M}_{\pi\sigma} \mathbf{e}_j$ så $\mathbf{M}_\pi \mathbf{M}_\sigma = \mathbf{M}_{\pi\sigma}$

Multiplikation i S_n motsvarar matrismultiplikation.

$$\mathbf{M}_\pi^t = \mathbf{M}_\pi^{-1} \quad (\text{ortogonal matris}) = \mathbf{M}_{\pi^{-1}}$$

Cayleys sats:

Varje grupp G är isomorf med en delgrupp till S_G .

Ty: $\varphi : G \rightarrow S_G$ så att för $g, h \in G : \varphi(g)(h) = gh$ då

$$(\varphi(g_1) \circ \varphi(g_2))(h) = \varphi(g_1)(\varphi(g_2)(h)) =$$


$$= \varphi(g_1)(g_2h) = g_1(g_2h) =$$

$$= (g_1g_2)(h) = \varphi(g_1g_2)h \quad \text{så}$$

$$\varphi(g_1) \circ \varphi(g_2) = \varphi(g_1g_2)$$

$$\varphi \text{ injektiv ty } g_1h = g_2h \Rightarrow g_1 = g_2$$

$$\text{så } G \cong \varphi(G) = \{\varphi(g) \mid g \in G\}$$

 Isomorfi, skrivs ibland $G \approx \varphi(G)$.

(Speciellt kan varje ändlig grupp representeras med matriser.)

Ordningen för $\pi \in S_n$ är lätt att se av π :s cykelstruktur.

$$\text{Exempel: } S_{12} \ni \pi = (1 \ 7 \ 4 \ 11)(2 \ 9 \ 6)(3 \ 5 \ 8 \ 12 \ 10)$$

$$o(\pi) = ?$$

$$4, 3, 5 \mid o(\pi) \quad \text{I varje cykel skall man gå ett helt antal varv.}$$

$$\text{"så"} \quad o(\pi) = \text{mgm}(4, 3, 5) = 60$$

Konjugering i S_n

$\alpha, \beta \in S_n$ är konjugerade om det finns $\sigma \in S_n$ så att $\sigma\alpha\sigma^{-1} = \beta$ (det vill säga $\sigma\alpha = \beta\sigma$).

En ekvivalensrelation på S_n (reflexiv, symmetrisk och transitiv).

Exempel:

$\sigma = (1\ 2\ 3)(4\ 5)$ är konjugerad till $\beta = (1\ 3)(2\ 4\ 5)$.

$\sigma = (1\ 5\ 3\ 4)$ ger $\sigma\alpha\sigma^{-1} = (1\ 5\ 3\ 4)(1\ 2\ 3)(4\ 5)(1\ 4\ 3\ 5) = (1\ 3)(2\ 4\ 5)$

Sats: $\alpha, \beta \in S_n$ är konjugerade om de har samma cykelstruktur.

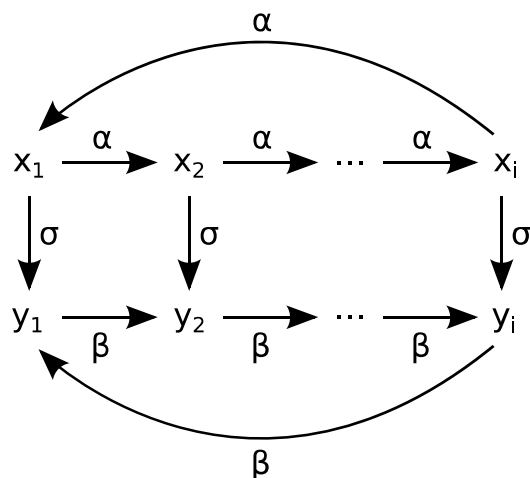
Samma antal i -cykler, alla i .

Ty: \Rightarrow : Om $\beta = \sigma\alpha\sigma^{-1}$ och α innehåller cykeln $(x_1\ x_2\ \dots\ x_i)$, innehåller β cykeln $(\sigma(x_1)\ \sigma(x_2)\ \dots\ \sigma(x_i))$.

\Leftarrow : Om $(x_1\ x_2\ \dots\ x_i)$ i α motsvarar $(y_1\ y_2\ \dots\ y_i)$ i β .

(Samma resonemang åt andra hållet.)

Så tar vi σ så att $\sigma(x_1) = y_1, \sigma(x_2) = y_2, \dots$, det ger $\beta = \sigma\alpha\sigma^{-1}$.



Klasser av konjugerade element i S_n svarar precis mot partitioner av heltalet n .

Exempel: Alla element i S_5 konjugerade med $(1\ 4)(2\ 5\ 3)$ är de med cykelstruktur $[2\ 3]$.

Exempel: $\underbrace{\sigma\pi}_\beta = \sigma \underbrace{(\pi\sigma)}_\alpha \sigma^{-1}$, så $\sigma\pi$ och $\pi\sigma$ är konjugerade.

En grövre uppdelning av S_n : jämna och udda.

En transposition: en permutation av typ $[1^{n-2}\ 2]$, det vill säga (ij) $i \neq j$.

Om $\pi \in S_n$ så finns transpositioner τ_1, \dots, τ_r så att $\pi = \tau_r \tau_{r-1} \dots \tau_2 \tau_1$
ty $(x_1\ x_2 \dots x_k) = (x_1\ x_k)(x_1\ x_{k-1}) \dots (x_1\ x_2)$.

π är en jämn/udda permutation om r är jämnt/udda då $\pi = \tau_r \tau_{r-1} \dots \tau_1$;
 $\text{sgn } \pi = (-1)^r$.

Sats:

Om $\pi \in S_n$, $\pi = \tau_r \tau_{r-1} \dots \tau_1 = \tau'_r \dots \tau'_1$ (τ_i, τ'_i transpositioner)
så har r och r' samma paritet. (Båda jämna eller båda udda.)

2011-(03)mar-29: dag 6, 18

Idag övning, men först en sak från föreläsning.

Sats:

Om $\pi \in S_n$ och $\pi = \tau_r \tau_{r-1} \dots \tau_1 = \tau'_{r'} \dots \tau'_2 \tau'_1$
(där π :na är transpositioner, det vill säga $= (ij)$, $i \neq j$).

Så har r och r' samma paritet (det vill säga båda udda eller båda jämna).

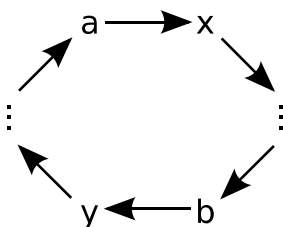
Ty:

Om $\sigma \in S_n$, τ en transposition i S_n ,
Låt $c(\sigma)$ vara antalet cykler i σ .
Vad blir $c(\sigma\tau)$?

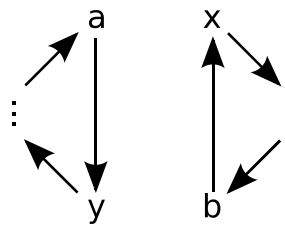
($\tau = ab$)

1) a, b i samma cykler i σ :

i σ :



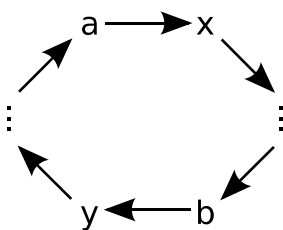
i $\sigma\tau$:



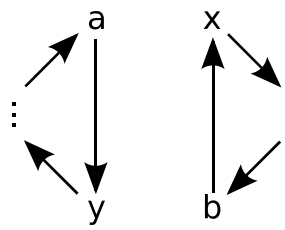
så $c(\sigma\tau) = c(\sigma) + 1$

2) a, b i olika cykler i σ :

i σ :



i $\sigma\tau$:



så $c(\sigma\tau) = c(\sigma) - 1$

Så $c(\pi) = c(\text{id } \tau_r \dots \tau_2 \tau_1) = c(\text{id } \tau'_{r'} \dots \tau'_2 \tau'_1)$
ger att r och r' har samma paritet.

Oberservera att tecknet för π , $\text{sgn } \pi =$

$$= (-1)^r = \begin{cases} 1 & \pi \text{ jämn} \\ -1 & \pi \text{ udda} \end{cases}$$

$$\text{sgn}(\pi\sigma) = \text{sgn } \pi \cdot \text{sgn } \sigma$$

$$\text{sgn } \pi^{-1} = \text{sgn } \pi$$

$$\text{sgn}(\sigma\alpha\sigma^{-1}) = \text{sgn } \alpha \quad \text{samma paritet i hela konjugatklassen (det vill säga samma cykelstruktur).}$$

$$\text{sgn}(x_1 \dots x_k) = (-1)^{k-1}$$

$$(x_1 \dots x_k) = \underbrace{(x_1 x_k)(x_1 x_{k-1}) \dots (x_1 x_2)}_{k-1 \text{ styck}}$$

$$\text{Om } \pi \text{ har typ } [1^{\alpha_1} 2^{\alpha_2} \dots k^{\alpha_k}] \text{ är } \text{sgn } \pi = (-1)^{\alpha_2 + \alpha_4 + \dots} = (-1)^{n - c(\pi)}$$

$$1) \quad \varphi, \psi \in S_n \quad \varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 8 & 5 & 2 & 4 & 3 & 7 \end{pmatrix},$$

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 4 & 1 & 2 & 6 & 3 & 5 \end{pmatrix}$$

$$\begin{aligned} \text{a)} \quad & \text{I cykeform: } \varphi = (1 \ 6 \ 4 \ 5 \ 2)(3 \ 8 \ 7), \\ & \psi = (1 \ 7 \ 3 \ 4)(2 \ 8 \ 5)(6) \end{aligned}$$

$$\text{b)} \quad \varphi\psi \text{ i tvåradform:}$$

$$\varphi\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 4 & 1 & 2 & 6 & 3 & 5 \\ 3 & 7 & 5 & 6 & 1 & 4 & 8 & 2 \end{pmatrix} \begin{matrix} \varphi \\ \psi \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 6 & 1 & 4 & 8 & 2 \end{pmatrix}$$

i cykelform:

$$\phi\psi = (1\ 6\ 4\ 5\ 2)(3\ 8\ 7)(1\ 7\ 3\ 4)(2\ 8\ 5) = (1\ 3\ 5)(2\ 7\ 8)(4\ 6)$$

$$\psi\phi = (1\ 7\ 3\ 4)(2\ 8\ 5)(1\ 6\ 4\ 5\ 2)(3\ 8\ 7) = (1\ 6)(2\ 7\ 4)(3\ 5\ 8)$$

$$\phi^{-1} = \begin{pmatrix} 6 & 1 & 8 & 5 & 2 & 4 & 3 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = (1\ 2\ 5\ 4\ 6)(3\ 7\ 8)$$

(eller (2\ 5\ 4\ 6\ 1)(7\ 8\ 3))

c)

$$\mathbf{M}_\phi = \begin{pmatrix} 0 & 1 & & & \\ 0 & & & & \\ 0 & & & & \\ 0 & & & & \\ 0 & & & & \\ 1 & & & & \\ 0 & & & & \\ 0 & & & & \\ 0 & & & & 1 \end{pmatrix}, \quad \mathbf{M}_\psi = \begin{pmatrix} 0 & & & & \\ 0 & & & & \\ 0 & & & & \\ 0 & & & & \\ 0 & & & & \\ 0 & & & & \\ 1 & & & & \\ 0 & & & & \end{pmatrix},$$

rad 6 rad 7

$$\mathbf{M}_{\phi\psi} = \begin{pmatrix} 0 & & & & \\ 0 & & & & \\ 1 & & & & \\ 0 & & & & \\ 0 & & & & \\ 0 & & & & \\ 0 & & & & \\ 0 & & & & \end{pmatrix} = \mathbf{M}_\phi \mathbf{M}_\psi$$

2) $\pi \in S_9$: $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 6 & 5 & 4 & 9 & 2 & 3 & 8 \end{pmatrix}$

a) $o(\pi)$?

π i cykelform: $(1\ 7\ 2)(3\ 6\ 9\ 8)(4\ 5)$

3 4 2

Så $o(\pi) = \text{mgm}(3, 4, 2) = 12$

b) π som en produkt av transpositioner: (varje cykel för sig)

$\pi = (1\ 2)(1\ 7)(3\ 8)(3\ 9)(3\ 6)(4\ 5)$, 6 stycken transpositioner.

Så $\text{sgn } \pi = (-1)^6 = 1$, π är en jämn permutation.

Kan också ses:

$$\text{sgn } \pi = (-1)^{\alpha_2 + \alpha_4 + \dots} = (-1)^{1+1} = 1$$

$$= (-1)^{n - c(\pi)} = (-1)^{n-3} = 1$$

3) $\pi = (1\ 7\ 2)(3\ 6\ 9\ 8)(4\ 5)$ från förra uppgiften.
 $\sigma = (1\ 5\ 3\ 9\ 6\ 8)(2\ 4)$

Vi söker χ, ψ så att $\pi\chi = \sigma, \psi\pi = \sigma$.

$$\chi = \pi^{-1}\sigma = \underbrace{(1\ 2\ 7)(3\ 8\ 9\ 6)(4\ 5)}_{\pi^{-1}}(1\ 5\ 3\ 9\ 6\ 8)(2\ 4) = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$$

$$\psi = \sigma\pi^{-1} = (1\ 5\ 3\ 9\ 6\ 8)(2\ 4)(1\ 2\ 7)(3\ 8\ 9\ 6)(4\ 5) = (1\ 4\ 3)(2\ 7\ 5)(6\ 9\ 8)$$

$\chi\psi$ konjugerade, $\psi = \pi\chi\pi^{-1}$

4) "Patiensen"

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \end{array} \longrightarrow \begin{array}{ccc} 1 & 5 & 9 \\ 2 & 6 & 10 \\ 3 & 7 & 11 \\ 4 & 8 & 12 \end{array} \longrightarrow \begin{array}{ccc} 1 & 6 & 11 \\ 5 & 10 & 4 \\ 9 & 3 & 8 \\ 2 & 7 & 12 \end{array} \longrightarrow \dots$$

a) $\pi(i) = j$ om kortet i position i hamnar i position j .

$$\pi \in S_{12} \quad \pi = (1)(2\ 4\ 10\ 6\ 5)(3\ 7\ 8\ 11\ 9)(12)$$

Upprepat n gånger fås π^n , första gången vi kommer tillbaka till något läge är efter $o(\pi)$ gånger, det vill säga 5 gånger.

b) Med positionerna $0, 1, 2, \dots, 11$ istället.

$$\pi = (0)(1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ 10\ 8)(11)$$

Det vill säga $\pi(i) = 3i \pmod{11}$ (förutom för (11))

så $o(\pi) = o(3)$ i $U(\mathbb{Z}_{11})$

$$|U(\mathbb{Z}_{11})| = 10 \text{ så } o(3) = 1, 2, 5 \text{ eller } 10.$$

$$3^1 = 3, \quad 3^2 = 9, \quad 3^5 = 1$$

$$o(\pi) = o(3) = 5$$

c) m rader, n kolonner

$$\begin{array}{ccccc} 0 & 1 & 2 & \dots & n-1 \\ n & n+1 & \dots & \dots & 2n-1 \\ 2n & \dots & \dots & \dots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ (m-1)n & \dots & \dots & \dots & (mn-1) \end{array} \mapsto \begin{array}{cccc} 0 & m & \dots & (n-1)m \\ 1 & m+1 & \dots & \vdots \\ 2 & m+2 & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ m-1 & 2m+1 & \dots & nm-1 \end{array}$$

”Tydliggen” $\pi(i) = ni \pmod{mn-1}$ $m \mapsto 1$

Ty $0 \mapsto 0$, ökar med n för varje steg till $m-1 \mapsto (m-1)n$

Så $o(\pi) = o(n)$ i $U(\mathbb{Z}_{mn-1})$.

d) Riffelblanding av en kortlek

$$\begin{array}{cc} 0\ 1 & 0\ 26 \\ & \swarrow \\ 2\ 3 & 1\ 27 \\ & \swarrow \\ 4\ 5 & 2\ 28 \\ & \swarrow \\ \vdots & \end{array} \mapsto \begin{array}{cc} 0 & 0 \\ 1 & 26 \\ 2 & 1 \\ 3 & 27 \\ \vdots & 3 \\ & 28 \\ & \vdots \end{array}$$

Fallet med samma kort överst och underst hela tiden:

$$m = 25, n = 2 \text{ ovan, det vill säga } \pi(i) = 2i \pmod{51}$$

Antalet gånger riffelblandningen måste upprepas för att ge samma läge.

$$o(\pi) = o(2) \text{ i } U(\mathbb{Z}_{51}) = \{x \in \mathbb{Z}_{51} \mid \text{sgd}(x; 51) = 1\}$$

$$|U(\mathbb{Z}_{51})| = |x| \overset{= \mathbb{Z}_{51}}{\substack{- |A| - |B| + |A \cap B| \\ - |A \cup B|}} = 51 - 17 - 3 + 1 = 32$$

A — de som är delbara med 3
B — de som är delbara med 17

$o(2) \text{ i } U(\mathbb{Z}_{51})$ är alltså 1, 2, 4, 8, 16 eller 32.

$$2^1 = 2, 2^2 = 4, 2^4 = 16, 2^8 = 256 = 1 \pmod{51}$$

så $o(2) = 8$ och
8 riffelblandningar av denna typ leder tillbaks.

Fall 2:

Inget kort orörligt. Fallet $m = 22, n = 2$.
(Fiktiva kort överst och underst.)

Antalet upprepningar till ursprungsläget:

$$\text{Detta fall: } o(2) \text{ i } U(\mathbb{Z}_{54-1}) = U(\mathbb{Z}_{53}) \quad \{53, \text{primit}\}$$

$$o(2) \setminus |U(\mathbb{Z}_{53})| = 52 = 2^2 \cdot 13$$

$$\text{Så } \begin{aligned} o(2) &= 1, 2, 4, 13, 26, 52 \\ o(2) &= 52 \end{aligned}$$

2011-(03)mar-31: dag 7, 19

Första delen på denna dag.

Sats: I S_n ($n \geq 2$) är hälften av permutationerna jämna och hälften udda.

Ty: En bijektion $\text{jämna} \leftrightarrow \text{udda}$ ges av

$f(\pi) = \pi\tau$, τ en transposition i S_n , tar udda till jämna och vice versa.

finns om $n \geq 2$

Bijektion ty $f^2 = \text{id} \Leftrightarrow f = f^{-1}$.

Determinanter:

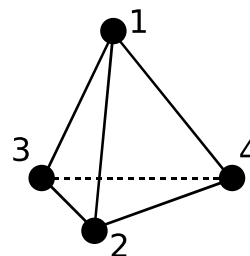
$$\det_{n \times n} A = \sum_{\pi \in S_n} \text{sgn } \pi \cdot a_{\pi(1)1} a_{\pi(2)2} \cdots a_{\pi(n)n}$$

Ö6:5)

Tetraeder (regelbunden)

Stella avbildningar (symmetrier för tetraederna)
motvistar element i $G = S_4$; permutationer av hörnen.

Konjugatklasser: a motsvarar typer av symmetrier.



Klass	antal	paritet	exempel	typ av avbildning
$[1^4]$	1	jämna	id	identitetsavbildningen
$[1^2 2]$	$\binom{4}{2} = 6$	udda	$(1\ 2)$	spegling i ett plan genom 34
$[2^2]$	3	jämn	$(1\ 2)(3\ 4)$	rotation π kring en axel genom mitten av 12 och mitten av 34

Klass	antal	paritet	exempel	typ av avbildning
[1 3]	8 4 sätt att välja ettan, 2 sätt att kombinera trean.	jämn	(1 2 3)	rotation $\pm \frac{2}{3}\pi$ kring en axel genom 4.
[4]	$3 \cdot 2 = 6$	udda	(1 2 3 4)	rotation kring $\pm \frac{1}{2}\pi$ kring en axel genom 13, 24:s mitt och spegling

- b) Jämna: rotationer (1 + 3 + 8 = 12 stycken)
 Udda: innehåller spegling (6 + 6 = 12 stycken)

- c) $N = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
 är sluten under \cdot (...), så delgrupp och

$$(1\ 2)N = \{(1\ 2), (3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\} = N(1\ 2)$$

På samma sätt: $\underbrace{gN = Ng}_{gNg^{-1} = N} \text{ för alla } g \in G.$

Så N är en normal grupp.

Kvotgruppen: $G/N = \{gN : g \in G\}$

Multipikation: $g_1Ng_2N = g_1g_2N$

Man finner:

$$G/N \cong S_n$$

Modul 4

2011-(03)mar-31: dag 1, 19

Andra delen på denna dag.

Felrättande koder

En binär kod $\mathcal{C} \subseteq \mathbb{Z}_2^n$ ($\mathbb{Z}_2 = \{0, 1\}$)
 n är kodens längd.

Exempel: $\mathcal{C} = \{001, 010, 110\}$

Viktiga egenskaper för en kod:

Hur många fel koden säkert kan upptäcka.

Hur många fel koden säkert kan rätta.

\mathcal{C} ovan kan inte upptäcka 1 fel:

010 med ett fel kan bli 110, ett kodord.

Men $\mathcal{C} = \{0010, 0100, 0111, 1011\}$ kan upptäcka ett fel
och $\mathcal{C} = \{010, 101\}$ kan rätta ett fel.

Minimala avståndet för koden \mathcal{C} :

$$\delta = \min\{d(a, b) : a, b \in \mathcal{C}, a \neq b\}$$

antalet positioner i med $a_i \neq b_i$

Koder kan upptäcka $\delta - 1$ fel och rätta e fel om $\delta \geq 2e + 1$,
det vill säga upp till $\left\lfloor \frac{\delta - 1}{2} \right\rfloor$ fel.

Exempel:

Givet $x, y \in \mathbb{Z}_2^n$, $n \geq 2$

$$x = 01001 \in S_2(x)$$

$$y = 11000 \in S_2(x)$$

Låt $S_2(x)$ = mängden ord (element i \mathbb{Z}_2^n) som fås från x med högst 2 fel.

$$S_2(x) = 1 + n + \binom{n}{2} = 1 + n + \frac{n(n-1)}{2} = \frac{1}{2}(n^2 + n + 2)$$

fel: 0 1 2

Visa att om E är en kod av längd $n = 8$ som rättar 2 fel så är $|E| \leq 6$.

Inget ord skall kunna fås med högst två fel från två olika kodord så

$$|E||S_2(x)| \leq 2^8 = 256$$

$$\{ \quad |S_2(x)| = \frac{1}{2}(8^2 + 8 + 1) = 37 \quad \}$$

$$|E| \leq \frac{256}{37} < 7 \quad |E| \leq 6$$

På samma sätt, sfärpackningssatsen:

Om koden \mathcal{C} av längd n rättar e fel:

$$|\mathcal{C}| \left(\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{e} \right) \leq 2^n$$

Mer systematiskt (algebraiskt)

\mathcal{C} är en linjär kod om

$$a, b \in \mathcal{C} \Rightarrow a + b \in \mathcal{C}$$

Addition position för position i \mathbb{Z}_2

+	0	1
0	0	1
1	1	0

Exempel:

$$11010 + 01110 = 10100$$

Detta betyder att \mathcal{C} är ett delrum (delgrupp) till \mathbb{Z}_2^n .

Så

$$|\mathcal{C}| \mid 2^n \quad \text{det vill säga } |\mathcal{C}| = 2^k \text{ för något } k \text{ (}\mathcal{C}\text{:s dimension)} \in \mathbb{N}$$

I en linjär kod:

$$\delta = \omega_{\min} = \min\{\omega(c) : c \in \mathcal{C}, c \neq 00\dots 00\}$$

vikten för c , det vill säga antalet 1:or i c

Ty:

$$\omega_{\min} = \omega(c^*) = d(c^*, 0) \geq \delta$$

och

$$\delta = d(c_1, c_2) = \omega(c_1 + c_2) \geq \omega_{\min}$$

2011-(04)apr-06: dag 2, 20

Enkelt sätt att hitta fel i en kod:

paritetskontrollbit (jämför med sista siffran (paritetssiffra) i personnummer).

670723-146

↓

12, 7, 0, 7, 4, 3, 2, 4, 12

↓

1, 2, 7, 0, 7, 4, 3, 2, 4, 1, 2 Summa: 33

$$33 + \underline{7} = 40 \equiv 0 \pmod{10}$$

↓

670723-1467

Lite allmännare:

(paritets)kontrollmatris

$$H = \underbrace{\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 \\ \vdots & & & & & & & & \end{pmatrix}}_n \Bigg\}^m \quad m \times n \text{ 0/1-matris}$$

Till H hör en linjär kod

$$\mathcal{C} = \{x \in \mathbb{Z}_2^n : \underbrace{Hx}_{(m \times n)x = n \times 1} = \underbrace{0}_{n \times 1}\} \quad \text{med dimension } n - \text{rank } H$$

antalet linjärt oberoende rader i H .

Enkelt fall:

$$H = \begin{pmatrix} I & B \\ m \times m & m \times (n - m) \end{pmatrix}$$

Sista $(n - m)$ positionen kan väljas fritt.

$$\text{Vad är } \mathcal{C} \text{ om } H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} ?$$

x_2 och x_4 kan vara godtyckliga,

då bestäms x_1, x_3 :

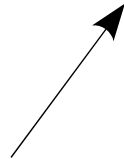
$$x_1 + x_2 + x_4 = 0 \Rightarrow x_1 = x_2 + x_4$$

$$x_2 + x_3 = 0 \Rightarrow x_3 = x_2$$

(i \mathbb{Z}_2)

$$\mathcal{C} = \{0000, 1001, 1110, 0111\}$$

x_2 :	x_4 :
0	0
0	1
1	0
1	1



Sats: Om H inte har någon kolonn $= 0$ samt att alla kolonner är unika, så rättar \mathcal{C} ett fel.



Koden som ges av H .

Ty: Vi skall se att $\omega_{\min} \geq 3$

$Hc = 0$ och $\omega(c) = 1$ skulle ge nollkolonn i H .
 $Hc = 0$ och $\omega(c) = 2$ ger två lika kolonner.

Med sådana H är det lätt att rätta ett fel (på position i)

Om vi tar emot $z_{n \times 1} = c + e = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

← rad i

↑
kodord i koden

Så $H z = H c + H e = H$:s i :te kolonn.



$= 0$ eftersom c är ett kodord

Exempel:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \quad \text{rättar enligt stsen minst ett fel.}$$

Vi tar emot $z = 11011$, vad sändes?
(Förutsätt att bara ett fel uppstod.)

$$Hz = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = H:s \text{ första kolonn}$$

Så första biten (siffran) är fel. $\Rightarrow c = 01011$

Hammingkod: H med alla kolonner unika och inte 0.

$$\underbrace{r \times (2^r - 1)}_{\text{Maximal bredd}}$$

Exempel:

$$r = 2 \\ 2^r - 1 = 3$$

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

r stycken ger x_1, x_2, \dots, x_r uttryckta i resten.

$$\text{Dimension: } k = 2^r - r - 1$$

$$\text{Minsta avstånd: } \delta = 3$$

$$\text{Längd: } n = 2^r - 1$$

$$|C| = 2^k = 2^{2^r - r - 1}$$

Sfärpackningssatsen med $e = 1$:

$$|C| \left(1 + \binom{n}{1} \right) \leq 2^n$$

\Downarrow

$$2^{2^r - r - 1} \cdot \underbrace{(1 + n)}_{2^r} \leq 2^n$$

\Downarrow

$$\underbrace{2^{2^r - 1}}_{2^n} \leq 2^n$$

\Downarrow

$$2^n \leq 2^n \quad \begin{array}{l} \text{Likhet!} \\ \text{Perfekta koder.} \end{array}$$

Exemplet:

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad \begin{array}{l} Hx = 0 \\ \text{ger: } C = \{000, 111\} \end{array}$$

$$\begin{array}{c} Hx = 0 \\ \left(\begin{array}{ccc|c} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{array} \right) \Leftrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array} \right) \end{array}$$

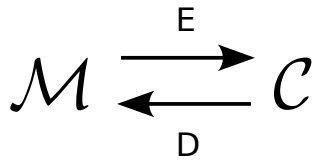
$$\begin{array}{ll} H \text{ ger:} & x_2 + x_3 = 0 \quad (\text{rad 1}) \\ & x_1 + x_3 = 0 \quad (\text{rad 2}) \end{array}$$

$$\begin{array}{ll} \text{Alltså:} & \begin{array}{l} \text{Antingen} \quad x_2 = 1 \Rightarrow x_3 = 1 \ \& \ x_1 = 1 \\ \text{eller} \quad \quad x_2 = 0 \Rightarrow x_3 = 1 \ \& \ x_1 = 1 \end{array} \end{array}$$

Kryptering (mest RSA)

Koder för att skydda information från obehöriga

Allmänt:



\mathcal{M} — Meddelandet i klartext

\mathcal{C} — Chiffer, krypterad text

E — Kryptering

D — Dekryptering (avkryptering)

$$D = E^{-1}$$

Klassiskt chiffer: byta bokstäver,
vanligtvis måste då E och D vara hemliga.

Ny idé: (Diffie, Hellman, 1976)

Offentlig nyckel E : allmänt känd, men så pass komplicerad
att det är svårt(!) att bestämma inversen, D .

Kallas envägsfunktion.

Exempel på sådant system:

RSA (Rivest, Shamir Adleman)

Simon Singh: Kodboken (☺)

Fermats lilla sats är grunden till RSA.

Fermats lilla sats

Om p är ett primtal och $a \in \mathbb{Z}_p \setminus \{0\}$:

$$a^{p-1} = 1 \quad \text{i } \mathbb{Z}_p \quad (a^{p-1} \equiv 1 \pmod{p})$$

$$\begin{aligned} p \nmid a &\Rightarrow p \mid a^{p-1} - 1 \quad \text{i } \mathbb{Z} \\ p \mid a^p - a &\quad \text{alla } a \end{aligned}$$

Exempel:

$$5^6 = \{5^6 = 5^{7-1}\} = 15625 = 2232 \cdot 7 + 1$$

Ty: $a \in \mathbb{Z}_p \setminus \{0\}$

En grupp med multiplikation, med $p - 1$ stycken element.
Så $a^{p-1} = 1$ i \mathbb{Z}_p .

Följdsats:

Låt p, q vara olika primtal

$$n = pq, m = (p - 1)(q - 1)$$

$$s \equiv 1 \pmod{m} \Rightarrow x^s \equiv x \pmod{n} \quad \text{för alla } x \in \mathbb{Z}$$

Ty:

$$s = 1 + k(p - 1)(q - 1), \text{ något heltal } k$$

$$\begin{aligned} x^s - x &= x(x^{k(p-1)(q-1)} - 1) = x((x^{p-1})^{(q-1)k} - 1) \equiv \\ &\equiv x(1^k - 1) = x(1 - 1) = x \cdot 0 = 0 \end{aligned} \quad (\text{mod } p, q)$$

$$p, q \nmid x^s - x \quad \text{så} \quad n = pq \nmid x^s - x$$

dualprimtal

RSA-systemet på på satsen:

Tag två olika stora(!) primtal, p, q . ($\sim 10^{150}$)

Beräkna $n = pq$, $m = (p - 1)(q - 1)$

Välj e med $\text{sgd}(e, m) = 1$ och

finn d med $ed \equiv 1 \pmod{m}$ (Euklides' algoritm)

Offentliggör n och e , men hemlighåll d (kasta m).

$$E(x) \equiv x^e \pmod{n} \quad E : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

$$D(x) \equiv x^d \pmod{n} \quad D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

$$\text{Gäller enär } D(E(x)) \equiv (E(x))^d \equiv (x^e)^d = x^{ed} \equiv x \pmod{n}$$

$$\therefore D(E(x)) = E(D(x))$$

E är en envägsfunktion (gör det klurigt) ty det är (troligen) svårt att primtalsfaktorisera stora tal.

Elektronisk signatur

B skickar till A:

$$E_A(D_B(x)) \text{ eller } D_B(E_A(x))$$

För att läsa det gör A:

$$D_A(E_A(D_B(x))) = D_B(x) \text{ och så:}$$

$$E_B(D_B(x)) = x \quad (E_B \text{ är offentlig})$$

Kan läsas bara av den som har tillgång till D_A (alltså A) och bara skrivits av den med D_B (alltså B).

Alternativt:

Offentliggör $D(x)$, alla kan läsa med E ,
men bara den som hade D kunde ha skrivit det.

Hur får man tag i stora primtal, p, q?

Det finns ganska gott om primtal.
Sannolikheten för att ett tal ska vara primtal:

$$\text{täthet} \sim \frac{1}{\ln n}, \quad n = \text{längden av talet}$$

det svåra är dock att känna igen dem, hur gör vi?

Primalitetstest

Pröva faktorer $(\sqrt{n} \approx 10^{75})$

Fermats lilla sats!

Fermattestet:

(Med bas b) för primalitet hos N

Är $b^{N-1} \equiv 1 \pmod{N}$?

Nej: N sammansatt, ej primtal.

Ja: Vi vet inte säkert.

Pseudoprimtal (bas b)

Sammansatta tal som klarar testet

Till exempel för bas 2:

$$341 = 11 \cdot 31$$

2011-(04)apr-07: dag 3, 21

3) Kodens längd n

Sfärpackningssatsen

$$4 \underbrace{\left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} \right)}_{\frac{1}{2}(n^2 + n + 2)} \leq 2^n$$

Det vill säga

n :	$n^2 + n + 2$	\leq	2^{n-1}
1	4		1
2	8		2
3	14		4
4	22		8
5	32		16
6	44		32
7	58		64

Så sfärpackningssatsen ger $n \geq 7$.

Men om c_1, c_2 av längd 7 har avstånd minst 5 (för två felrättningar) till c_3 kan avståndet mellan c_1 och c_2 inte vara > 4 :

Låt $A = \{\text{Positioner där } c_1 \text{ och } c_3 \text{ skiljer sig}\}$
 $B = \{\text{Positioner där } c_2 \text{ och } c_3 \text{ skiljer sig}\}$

$$d(c_1, c_2) = |(A \cup B) \setminus (A \cap B)| = |A \cup B| - |A \cap B| \leq 4$$

$$\text{men } |A \cup B| - |A \cap B| = \underbrace{|A|}_{\leq 7} + \underbrace{|B|}_{\geq 5} - \underbrace{|A \cap B|}_{\substack{\uparrow \\ \text{så } \geq 3}} \geq 5 - 3 = 2$$

7 räcker inte, men med $n = 8$

$$\mathcal{C} = \{00000000, 11111000, 00011111, 11100111\}$$

4)

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \xrightarrow[r4+r2]{r3+r1} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{r1+r4} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \xrightarrow[r3+r4]{r1+r3} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = H_1$$

H och H_1 definierar samma linjär kod \mathcal{C} .
 Linjärt oberoende rader så $\text{rang } H = 4$.

a) Antalet ord i \mathcal{C} , $|\mathcal{C}| = 2^k = 2^{n - \text{rang } H} = 2^{8-4} = 16$

c) Antalet ord inte i \mathcal{C} :

$$2^8 - |\mathcal{C}| = 256 - 16 = 240$$

d) Ett sådant ord: 00100111

e) Felaktiga ord med ett fel:

$$16 \cdot 8 = 128 \text{ stycken}$$

f) Rätta ordet 01111000

$$Hz = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = H\text{'s 5:e kolonn}$$

Så det rättade ordet (ett fel): 01110000

- 5) Om H har en m linjärt oberoende rader skall $n = 7 + m$ ty dimensionen $k = n - \text{rank } H = 7 - m$.

1-felrättande om alla kolonner olika $\neq \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad 128 = 2^7$

Så $7 + m \leq 2^m - 1$

m	$8 + m$	\leq	2^m	
1	9		2	X
2	10		4	X
3	11		8	X
4	12		16	0 OK

Så minimala antalet rader i $H = 4$.
Kolonner: 11

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

- 8) RSA med $n = 77 = 7^p \cdot 11^q$

$$m = (p - 1)(q - 1) = 6 \cdot 10 = 60$$

a) Parametern $e = 45$ går ej ty $\text{sgd}(45, 6) = 13 \neq 1$

b) $e = 13$ går bra $\text{sgd}(13, 60) = 1$

Vad blir d ? ($ed \equiv 1 \pmod{m}$)

Euklides' algoritm:

$$60 = 4 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$1 = 3 - 2 =$$

$$= 3 - (5 - 3) =$$

$$= 2 \cdot 3 - 5 =$$

$$= 2(8 - 5) - 5 =$$

$$= 2 \cdot 8 - 3 \cdot 5 =$$

$$= 2 \cdot 8 - 3(13 - 8) =$$

$$= -3 \cdot 13 + 5 \cdot 8 =$$

$$= -3 \cdot 13 + 5(60 - 4 \cdot 13) =$$

$$= 5 \cdot 60 - 23 \cdot 13 =$$

$$= (5 - 13) \cdot 60 + (60 - 23) \cdot 13 =$$

$$= 37 \cdot 13 - 8 \cdot 60$$

Så $37 \cdot 13 \equiv 1 \pmod{60}$, vi har $d = 37$

c) $E(3) = 3^{13} = 3^8 \cdot 3^4 \cdot 3^1$

$$3^2 \equiv 9, \quad 3^4 = 9^2 \equiv 4, \quad 3^8 = 4^2 \equiv 16 \pmod{77}$$

$$E(3) \equiv 6 \cdot 4 \cdot 3 = 192 \equiv 36 \pmod{77}$$

Så $E(3) = 38$

d) $D(2) \equiv 2^{37} \equiv 2^{32} \cdot 2^4 \cdot 2 \equiv 4 \cdot 16 \cdot 2 = 128 \equiv 51 \pmod{77}$

1	2	4	8	16	32
2	4	16	25	9	4

11) Är 63 ett primtal?

Fermattest med bas 2

$$2^{62} \equiv ? \pmod{63}$$

$$2^{62} = 2^{32} \cdot 2^{16} \cdot 2^8 \cdot 2^4 \cdot 2^2$$

$$\begin{aligned} \text{mod } 63: \quad 2^2 &= 4 \\ 2^4 &= 4^2 = 16 \\ 2^8 &= 16^2 = 256 \equiv 4 \\ 2^{16} &= 4^2 = 16 \\ 2^{32} &= 16^2 \equiv 4 \end{aligned}$$

$$2^{64} \equiv 4 \cdot \underbrace{16 \cdot 4}_1 \cdot \underbrace{16 \cdot 4}_1 = 4 \pmod{63}$$

Ej primtal.

12) Vad är $43^{139702} \pmod{101}$?

101 är ett primtal och $101 \nmid 43$ så

$$43^{100} \equiv 1 \pmod{101} \quad \{\text{Fermats lilla sats}\}$$

Så:

$$43^{139702} = 43^{1307} \cdot 43^2 = 43^2 = 1849$$

$$18 \cdot 101 + 31 = 31$$

2011-(04)apr-12: dag 4, 22

Lite till

Primalitetstest

Fermattest

Pseudoprimtal, Carmichaeltal

Miller-Rabins test

Lite satslogik och boolesk algebra

Satslogik

Atomära sentenser

Konnektiven $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

Sanningsvärdestabeller

Logisk ekvivalens

Boolesk algebra

Räkneregler

Booleska funktioner

Disjunktiv och konjunktiv normalform

Minimering, Karnaughdiagram

Primtalstest

Är (det stora) talet N ett primtal?

Fermattest (bas b , $1 < b < N$):

Är $b^{N-1} \equiv 1 \pmod{N}$?

Nej: N är sammansatt. Ja: Vet inte.

Pseudoprimtal, bas b :

Sammansatt, klarar Fermattestet, bas b .

Exempel: $341 = 11 \cdot 31$, bas 2

Mer om primalitetstest

Problematiska för Fermattestet:

Carmichaeltal:

Klarar alla Fermattest med bas b med $\text{sgd}(b, N) = 1$.

Exempel:

$$N = 561 = 3 \cdot 11 \cdot 17, \quad 560 = 2^4 \cdot 5 \cdot 7$$

N är ett Carmichaeltal om det är kvadratfritt och
 $p \mid N \Rightarrow p - 1 \mid N - 1$.

Det finns oändligt många sådana

1105, 1729, 2465, ...

Starkare test:

Miller-Rabins test (M-R) (1980)

Förfinning av Fermattestet:

$$N - 1 = n \cdot 2^r, \quad n \text{ udda}, r \geq 1 \text{ (} N \text{ udda)}$$

M-R:

$$b^n \pmod{N}$$

$$(b^n)^2 \pmod{N}$$

$$\left((b^n)^2 \right)^2 = b^{n \cdot 2^2} \pmod{N}$$

\vdots

$$b^{n \cdot 2^r} \equiv 1 \pmod{N}$$

Om N klarar Fermattestet, bas b .

Om N är ett primtal:

$$b^n \equiv 1 \pmod{N}$$

eller

$$(b^n)^{2^i} \equiv -1 \pmod{N}, \quad \text{något } i, 0 \leq i < r.$$

Exempel: $N = 561$, bas $= 2$

$$N - 1 = 560 = 35 \cdot 2^4$$

$$2^{35} \equiv 263 \pmod{561}$$

$$2^{70} \equiv 263^2 \equiv 166 \pmod{561}$$

$$2^{140} \equiv 166^2 \equiv 67 \pmod{561}$$

$$2^{280} \equiv 67^2 \equiv 1 \pmod{561}$$

$$2^{56} \equiv 1 \pmod{561}$$



561 är inte ett primtal, ty detta är inte -1 .

$$561 = 3 \cdot 11 \cdot 17$$

Om -1 på alla rader så
så primtal.

mod	3	11	17	Faktorer
	-1	-1	10	
	1	1	13	
	1	1	-1	
	1	1	1	Vi är klara

Lite om satslogik

Studerar påstående "matematiskt".

Exempel:

"Lisa läser diskret matematik." : A

"Det regnar." : B

$\neg A$: "Lisa läser inte diskret matematik."

$A \wedge \neg B$: "Lisa läser diskret matematik och det regnar inte."

$C \rightarrow A \vee B$: "Om det är onsdag så läser Lisa diskret matematik eller
så regnar det (eller båda)."

Säger man "antingen A eller B" så menar man, men
"eller", "A, B, eller både A och B".

Operationerna för sammansatta påståenden kallas konnektiv.

\neg	negation	“inte”, “icke-”
\wedge	konjunktion	“och”, “men” (skillnaden får inte i den här analysen)
\vee	disjunktion	“eller”, “minst en av”
\rightarrow	implikation	“om ... så ...”, “bara om”
\leftrightarrow	dubbel implikation	“omm” (= “om och endast om”)

Deras betydelse ges av sanningsvärdestabeller:

p	$\neg p$	
1	0	1 = sant 0 = falskt
0	1	

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

$p \wedge q$:	1 omm båda 1	»båda sanna«
$p \vee q$:	0 omm båda 0	»någon sann«
$p \rightarrow q$:	0 omm (1, 0)	»q minst lika sann som p«
$p \leftrightarrow q$:	1 omm lika	»p och q lika sanna«

Sanningsvärdestabeller för "större" sentenser

A B C	$C \rightarrow (A \wedge \neg B)$ $C \rightarrow A \wedge \neg B$			$(C \rightarrow A) \wedge \neg(B \wedge C)$				
1 1 1	0	0	0	1	0	0	1	
1 1 0	1	0	0	1	1	1	0	
1 0 1	1	1	1	1	1	1	0	
1 0 0	1	1	1	1	1	1	0	
0 1 1	0	0	0	0	0	0	1	
0 1 0	1	0	0	1	1	1	0	
0 0 1	0	0	1	0	0	1	0	
0 0 0	1	0	1	1	1	1	0	
	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 2px;">0 1</div> <div>0 0</div> <div>0 1</div> </div> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div>hela</div> <div>$A \wedge \neg B$</div> <div>$\neg B$</div> </div>			<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 2px;">0 1</div> <div>0 1</div> <div>0 1</div> <div>1 0</div> </div> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div>$C \rightarrow A$</div> <div>hela</div> <div>$\neg(B \wedge C)$</div> <div>$B \wedge C$</div> </div>				(1)
								(2)
								(3)

Observera att i exemplet får båda sentenserna samma sanningsvärden i alla tolkningar (alla rader). Vi säger att sentenserna är logiskt ekvivalenta.

$$C \rightarrow A \wedge \neg B \equiv (C \rightarrow A) \wedge \neg(B \wedge C)$$

(⇔ i boken)

Exempel:

$$p \rightarrow q \equiv \neg q \rightarrow \neg p \quad (\text{kontraposition})$$

$$p \rightarrow q \not\equiv q \rightarrow p \quad (\text{omvändning})$$

Alla logiska ekvivalenser kan fås med några enkla "tanelagar" (algebraiska).

Boolesk algebra, enkla logiska ekvivalenser

$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$	kommutativitet
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	associativitet
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	distributivitet
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan
$p \wedge p \equiv p$	$p \vee p \equiv p$	idempotens
$p \wedge (p \vee q) \equiv p$	$p \vee (p \wedge q) \equiv p$	absorption

$\neg \neg p \equiv p$	involution
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$	\leftrightarrow uttryckt
$p \rightarrow q \equiv \neg p \vee q$	\rightarrow uttryckt
$\neg p \equiv p \rightarrow \perp$	\neg uttryckt

$p \wedge \neg p \equiv \perp$	komplementaritet
$p \wedge \perp \equiv \perp$	Alltid falsk (falsum)
$p \wedge \top \equiv p$	
	Alltid sann (verum)

Annat skrivsätt (x·y skrivs oftast xy)

$p \cdot q = q \cdot p$	$p + q = q + p$	kommutativitet
$(p \cdot q) \cdot r = p \cdot (q \cdot r)$	$(p + q) + r = p + (q + r)$	associativitet
$p \cdot (q + r) = (p \cdot q) + (p \cdot r)$	$p + (q \cdot r) = (p + q) \cdot (p + r)$	distributivitet
$\overline{\overline{p \cdot q}} = \overline{\overline{p}} \cdot \overline{\overline{q}}$	$\overline{\overline{p + q}} = \overline{\overline{p}} + \overline{\overline{q}}$	De Morgan
$p \cdot p = p$	$p + p = p$	idempotens
$p \cdot (p + q) = p$	$p + (p \cdot q) = p$	absorption

$\overline{\overline{p}} = p$ involution

$p \cdot \overline{p} = \mathbf{0}$	komplementaritet
$p \cdot \mathbf{0} = \mathbf{0}$	
$p \cdot \mathbf{1} = p$	

Notera att $\overline{\overline{x} \cdot \overline{y}} \neq \overline{\overline{x}} \cdot \overline{\overline{y}}$ och $\overline{\overline{x} \cdot \overline{y}} \neq \overline{\overline{x} \cdot y}$

(Det som stod på förra sidan)

$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$	kommutativitet
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	associativitet
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	distributivitet
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan
$p \wedge p \equiv p$	$p \vee p \equiv p$	idempotens
$p \wedge (p \vee q) \equiv p$	$p \vee (p \wedge q) \equiv p$	absorption

$$\neg \neg p \equiv p \quad \text{involution}$$

$$\begin{aligned} p \wedge \neg p &\equiv \perp & \text{komplementaritet} \\ p \wedge \perp &\equiv \perp \\ p \wedge \top &\equiv p \end{aligned}$$

Motsvarande i mängdlära

$A \cap B \equiv B \cap A$	$p \cup q \equiv q \cup p$	kommutativitet
$(A \cap B) \cap C \equiv A \cap (B \cap C)$	$(p \cup q) \cup r \equiv p \cup (q \cup r)$	associativitet
$A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$	$p \cup (q \cap r) \equiv (p \cup q) \cap (p \cup r)$	distributivitet
$(A \cap B)^c \equiv A^c \cup B^c$	$(p \cup q)^c \equiv p^c \cap q^c$	De Morgan
$A \cap A \equiv A$	$p \cup p \equiv p$	idempotens
$A \cap (A \cup B) \equiv A$	$p \cup (p \cap q) \equiv p$	absorption

$$A^{c^c} \equiv A \quad \text{involution}$$

$$\begin{aligned} A \cap A^c &\equiv \emptyset & \text{komplementaritet} \\ A \cap \emptyset &\equiv \emptyset \\ A \cap \mathcal{U} &\equiv A \end{aligned}$$

[5.3] (Text om ett hypotetiskt reglemente finns nog i en av böckerna)

Exempel med "resonemang" (att förenkla logiska uttryck) med boolesk algebra.

Militärt reglement:

$$x \rightarrow y = \bar{x} + y$$

- a: slips skall bäras
- b: vapenrock skall bäras
- c: ytterrock skall bäras

Reglementet:

$$\begin{aligned} & (\bar{a} \rightarrow \bar{b})(a\bar{b} \rightarrow c)((c + \bar{a}) \rightarrow b) = \\ = & (\bar{a} + \bar{b})(\overline{a\bar{b}} + c)(\overline{c + \bar{a}} + b) = \\ = & (\bar{a} + \bar{b})(a + \bar{b} + c)(\bar{c} + a + b) = \\ = & (a + \bar{b})(\bar{a} + b + \bar{c})(a\bar{c} + b) = \\ = & (a + \bar{b})(b + (\bar{a} + \bar{c})a\bar{c}) = \\ = & (a + \bar{b})(b + \mathbf{0}c + a\bar{c}) = \\ = & (a + \bar{b})(b + a\bar{c}) = \\ = & ab + a\bar{c} + \mathbf{0} + a\bar{b}\bar{c} = \\ = & a(b + \bar{c} + \bar{b}\bar{c}) = \\ = & a(b + \bar{c}) = \\ = & a(c \rightarrow b) \end{aligned}$$

Så förenklingen:

- 1) Slips skall bäras.
- 2) Om ytterrock bäres, skall vapenrock bäras.

2011-(04)apr-14: dag 5, 23

Del 1, på denna dag!

Boolesk algebra

- Booleska funktioner

- Disjunktiv och konjunktiv normalform

- Logiska grindar och kretsar

- Minimering, Karnaughdiageran

Grafteori

- Grafer, exempel

- Grafteoretiska grundbegrepp

- Bipartita grafer

- Grannmatris och incidensmatris

- Isomorfi mellan grafer

- Valens (grad), reguljära grafer

- Vägar, stigar och sånt

- Eulervägar och -kretsar, Hamiltonstigar och -cykler

- Sammanhängande grafer, komponenter

0-ställiga (en. nullary) konnektiv: \perp \top

1-ställiga (en. unary) konnektiv: \neg

2-ställiga (en. binary) konnektiv: \wedge \vee \rightarrow \leftrightarrow

Två olika skrivsätt:

\cdot $+$ \neg **1** **0** $=$
 \wedge \vee \neg \top \perp \equiv

(eller \leftrightarrow)

Idag först mer om boolesk /bo:lsk/ algebra

Ett exempel till: $\mathbb{B}_n = \{0, 1\}^n = \underbrace{\{00\dots 0, 00\dots 1, \dots, 11\dots 1\}}_{\times n}$

$+$, \cdot definieras komponentvis:

$+$	0	1
0	0	1
1	1	1

\cdot	0	1
0	0	0
1	0	1

$$\overline{0} = 1$$

$$\overline{1} = 0$$

$+$ är inte likadan som i \mathbb{Z}_2 .

Exempel:

$$n = 3$$

$$010 + 011 = 011$$

Booliska funktioner

$$f : \{0, 1\}^n \rightarrow \{0, 1\} \quad (f : \mathbb{B}_n \rightarrow \mathbb{B})$$

Exempel:

Sentenser (med bara atomära sentenser bland n givna)

Exempel:

$$\neg(A \rightarrow \neg B)$$

definierar funktionen

$$\begin{aligned} f(1, 1) &= 1 \\ f(1, 0) &= 0 \\ f(0, 1) &= 0 \\ f(0, 0) &= 0 \end{aligned}$$

En boolesk funktion beskrivs fullständigt av en sanningsvärdestabell.

Exempel:

x	y	z	f(x, y, z)		
1	1	1	1	xyz	1 på denna rad, 0 för övriga
1	1	0	1	xy \bar{z}	1 på denna rad, 0 för övriga
1	0	1	1	x \bar{y} z	1 på denna rad, 0 för övriga
1	0	0	0		
0	1	1	0		
0	1	0	0		
0	0	1	1	$\bar{x}\bar{y}$ z	1 på denna rad, 0 för övriga
0	0	0	0		

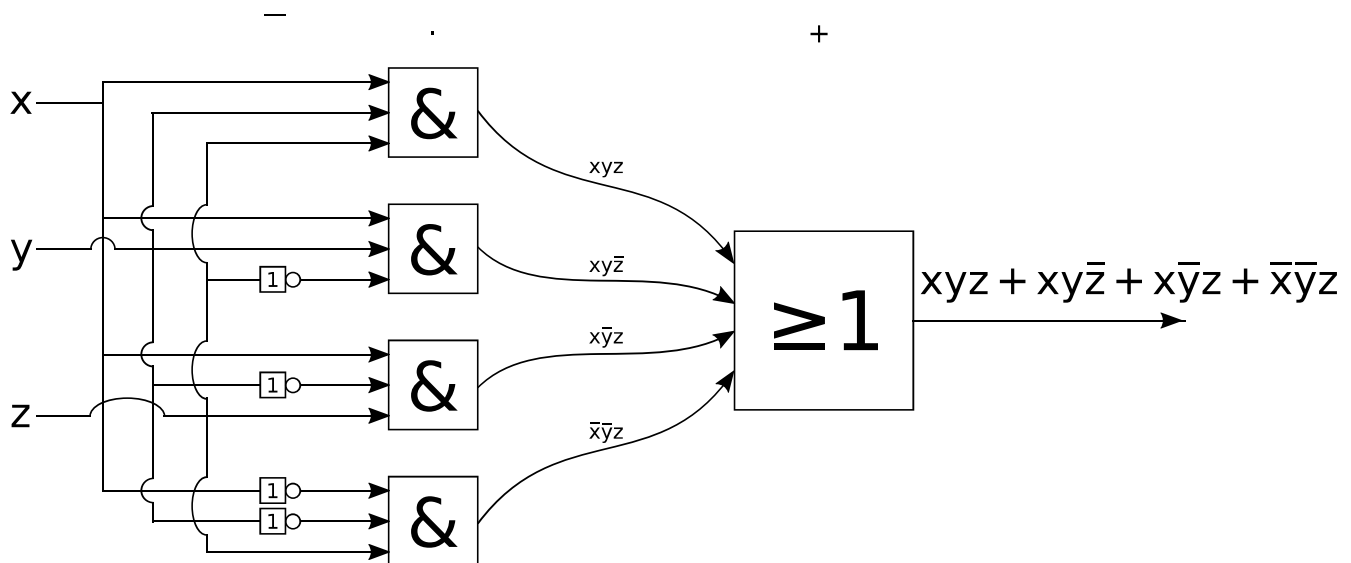
“Så” $f(x, y, z) = xyz + xy\bar{z} + x\bar{y}z + \bar{x}\bar{y}z$

På samma sätt kan varje boolesk funktion skrivas på disjunktiv normalform (dnf).

Dualt: konjunktiv normalform (knf)

$$f(x, y, z) = (\bar{x} + y + z)(x + \bar{y} + \bar{z})(x + \bar{y} + z)(x + y + z)$$

$f(x, y, z)$ kan "realiseras" med en logisk krets:



Uttrycket kan förenklas till en mindre, disjunktiv form.

Karnaugh-diagram

		Z	
		\bar{z}	z
xy	\bar{x}	00	0 1
	y	01	0 0
	x	11	1 1
	\bar{y}	10	0 1

Här är $f(x, y, z) = \underline{xy} + \underline{\bar{y}z}$

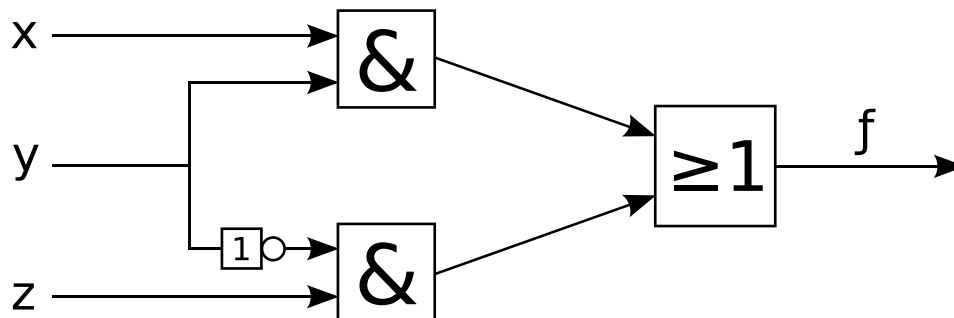
För ihop 1:orna i rektanglar med sida 1, 2 eller 4 (2^n). Rektanglarna ska vara Så stora som möjlig som får vara överlappande.

Endast en skillnad per rad i xy, gäller även i kolonnerna.

I diagrammet till vänster finns, det två ihopföringar, de heldragna bilder en rektangel.

Alltså:

En enklare krets för $f(x, y, z)$:



Ett exempel till:

Förenkla $f(x, y, z, w) = (\bar{x}\bar{y}\bar{z}\bar{w})_{(1)} + (\bar{x}\bar{y}z\bar{w})_{(2)} + (\bar{x}y\bar{z}w)_{(3)} + (xy\bar{z}\bar{w})_{(4)} +$
 $+ (xy\bar{z}w)_{(5)} + (x\bar{y}\bar{z}\bar{w})_{(6)} + (x\bar{y}\bar{z}w)_{(7)} + (x\bar{y}z\bar{w})_{(8)}$

Karnaughdiagram:

		ZW			
		00	01	11	10
xy	00	1 ₍₁₎	0	0	1 ₍₂₎
	01	0	1 ₍₃₎	0	0
	11	1 ₍₄₎	1 ₍₅₎	0	0
	10	1 ₍₆₎	1 ₍₇₎	0	1 ₍₈₎

"så" $f(x, y, z, w) = \boxed{x\bar{z}} + \boxed{\bar{y}\bar{w}} + \boxed{\bar{y}\bar{z}w}$

2011-(04)apr-27: dag 6, 24

Del 1, på denna dag!

KS 4 måndag V32, V34
Övning idag

1) Låt A: "Det är måndag", B: "Det snöar"

Är några av följande logiskt ekvivalenta?

α. "Att minst en av $\neg A$ och B gäller medgör att det inte är så att A om B."
Det vill säga:

$$(\neg A \vee B) \rightarrow \neg(B \rightarrow A)$$

β. "Det är inte så att båda A och A omm $\neg B$."
Det vill säga:

$$\neg(A \wedge (A \leftrightarrow \neg B))$$

γ. "Det är inte så att A omm B"
Det vill säga.

$$\neg(A \leftrightarrow B)$$

För att undersöka logisk ekvivalens ställer vi upp sanningsvärdestabell.

A	B	$\neg A \vee B \rightarrow \neg(B \rightarrow A)$					$\neg(A \wedge (A \leftrightarrow \neg B))$				$\neg(A \leftrightarrow B)$	
1	1	0	1	0	0	1	1	0	0	0	0	1
1	0	0	0	1	0	1	0	1	1	1	1	0
0	1	1	1	1	1	0	1	0	1	0	1	0
0	0	1	1	0	0	1	1	0	0	1	0	1
		①	②	③	②	①	④	③	②	①	②	①

Så $(\neg A \vee B) \rightarrow \neg(B \rightarrow A) \equiv \neg(A \wedge (A \leftrightarrow \neg B)) \neq \neg(A \leftrightarrow B)$

Logiskt ekvivalenta, ty samma på alla rader

Har andra sanningsvärden på minst en rad.

Alltså:

$\alpha \equiv \gamma$,
 $\beta \neq \alpha, \gamma$

Med boolesk algebra

(Minns att $a \rightarrow b = \bar{a} + b$)

$$\begin{aligned} a \leftrightarrow b &= (a \rightarrow b)(b \rightarrow a) = (\bar{a} + b)(\bar{b} + a) = \\ &= \bar{a}\bar{b} + \underbrace{\bar{a}a}_0 + \underbrace{b\bar{b}}_0 + ba = ab + \bar{a}\bar{b} \end{aligned}$$

$$\alpha = (\bar{a} + b) \rightarrow \overline{b \rightarrow a} = \overline{\bar{a} + b} + \overline{\bar{b} + a} = \bar{\bar{a}} \cdot \bar{b} + \bar{\bar{b}} \cdot \bar{a} = a \cdot \bar{b} + b \cdot \bar{a} = a \cdot \bar{b} + \bar{a} \cdot b$$

$$\begin{aligned} \beta &= \overline{a(a \leftrightarrow b)} = \overline{a(\bar{a}\bar{b} + \bar{a}b)} = \overline{a(\bar{a}\bar{b} + \bar{a}b)} = \bar{a} + \overline{\bar{a}\bar{b} + \bar{a}b} = \bar{a} + \overline{\bar{a}\bar{b}} \cdot \overline{\bar{a}b} = \\ &= \bar{a} + (\bar{a} + \bar{\bar{b}})(\bar{\bar{a}} + \bar{b}) = \bar{a} + (\bar{a} + b)(a + \bar{b}) = \bar{a} + \bar{a}a + \bar{a}\bar{b} + ba + b\bar{b} = \\ &= \bar{a} + \mathbf{0} + \bar{a}\bar{b} + ba + \mathbf{0} = \underbrace{\bar{a} + \bar{a}\bar{b}}_{\bar{a}} + ab = \bar{a} + ab = (\bar{a} + a)(\bar{a} + b) = \\ &= \bar{a} + b = a \rightarrow b \end{aligned}$$

$$\gamma = \overline{a \leftrightarrow b} = \overline{\bar{a}\bar{b} + \bar{a}b} = \overline{\bar{a}\bar{b}} \cdot \overline{\bar{a}b} = (\bar{a} + \bar{b})(a + b) = \bar{a}b + a\bar{b} = a\bar{b} + \bar{a}b$$

- 2) Visa med övriga boolesk algebralagar att $p + pq = p$ och $p(p + q) = p$.

$$p + pq = p\mathbf{1} + pq = p(\mathbf{1} \cdot q) = p\mathbf{1} = p \quad (1)$$

$$p(p + q) = (p + \mathbf{0})(p + q) = p + \mathbf{0}q = p + \mathbf{0} = p \quad \blacksquare$$

Alternativt:

$$p(p + q) = pp + pq = p + pq = \{(1)\} = p$$

4) Ge en minimal disjunktiv form för

a) $f(x, z) = xz + x\bar{z} + \bar{x}z$

Karnaughdiagram:

		z		
		0	1	
x	0	1	0	\bar{x}
	1	1	1	x
		\bar{z}	z	

Så: $\boxed{\bar{z}} + \textcircled{x}$

Alltså: $f(x, z) = x + \bar{z}$

b) $f(x, y, w) = \bar{x}y + \bar{x}\bar{y}\bar{w} + \bar{y}w =$

$$= \left\{ \begin{array}{c|cc} & 0 & 1 \\ \hline xy & 00 & 1 \\ & 01 & 1 \\ & 11 & 0 \\ & 10 & 0 \end{array} \right. + \begin{array}{cc} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{array} + \begin{array}{cc} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{array} =$$

$$= \left\{ \begin{array}{c|cc} & 0 & 1 \\ \hline xy & 00 & 1 \\ & 01 & 1 \\ & 11 & 0 \\ & 10 & 0 \end{array} \right\} = \boxed{\bar{x}} + \boxed{\bar{y}w}$$

2011-(04)apr-28: dag 7, 25

Del 1 på denna dag!

Mer om grafteori

Resten från övning 8.

Träd

Spännande träd

Minimala spännande träd, Kruskals algoritm

Binära rotade träd

Planära grafer

Eulers polyederformel

K_5 och $K_{3,3}$ är inte planära, Kuratowskis sats

Övnings-KS 4

Anmälan till tentan senast 15 maj.

Övnings-KS 4

1 a) $n = 46 = 2 \cdot 23, \quad m = (2 - 1)(23 - 1) = 22$

Krav: $\text{sgd}(e, m) = 1, \text{sgd}(2, 22) = 2$

b) $e = d = 5$

Möjligt om det finns primtal, p, q , med $e \cdot d \equiv 1 \pmod{(p - 1)(q - 1)}$.

$$p = 7, q = 3$$

$$e \cdot d = 25$$

$$(p - 1)(q - 1) = 6 \cdot 2 = 12$$

$$25 - 2 \cdot 12 = 1$$

Så: Ja.

d) Antalet ord: 2^k , k dimensioner. Längden $n = k + r$. r — H:s rang
8 ord $k = 3, n = 7$, så minst 4

e) $f(x_1, \dots, x_n)$

Antalet punkter (rader i värdetabellen): 2^n

totala antalet funktioner: 2^{2^n}

2 a)

$$H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Mottaget 111111

Vi försöker rätta:

$$H \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

Inte än kolonn, så inte ett fel, minst två fel.

b)

$$f(x, y, z) = xyz + xy\bar{z} + x\bar{y}z$$

Karnaughdiagram

		z	
		0	1
xy	00	0	0
	01	0	0
	10	1	1
	11	0	1

$$\text{Så } f(x, y, z) = x\bar{y} + xz$$

c) RSA med $n = 65$, finn möjligt e

$$n = 5 \cdot 13, \quad m = 4 \cdot 12 = 48$$

$$\text{Krav: } \text{sgd}(e, m) = \text{sgd}(2, 48) = 1$$

Till exempel: 5

$$3) \quad f(x, y, z) = (xy + \overline{(x + y)})z = (xy + \bar{x}\bar{y})z = xyz + \bar{x}\bar{y}z$$

5) Finn en kontrollmatris, H, till en 1-felrättande kod \mathcal{C} med 16 ord, så att $1011000 \in \mathcal{C}$.

$$n = 7, \quad 16 = 2^4, \quad \text{så } \dim k = 4$$

$$\text{så } H\text{'s rang} = r - k = 3$$

H av typ 3×7 , alla kolonner olika $\neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

Villkoret att $1011000 \in \mathcal{C}$ get att summan av kolonn 1, 3, 4 är $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

Till exempel:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}_1 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}_3 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}_4, \quad \text{fyll på med olika kolonner.}$$

$$\text{Till exempel:} \quad H = \begin{matrix} & \downarrow & & \downarrow & \downarrow & & \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \end{matrix}$$

Modul 5

2011-(04)apr-14: dag 1, 23

Del 2, på denna dag!

Boolesk algebra

- Booleska funktioner

- Disjunktiv och konjunktiv normalform

- Logiska grindar och kretsar

- Minimering, Karnaughdiageran

Grafteori

- Grafer, exempel

- Grafteoretiska grundbegrepp

- Bipartita grafer

- Grannmatris och incidensmatris

- Isomorfi mellan grafer

- Valens (grad), reguljära grafer

- Vägar, stigar och sånt

- Eulervägar och -kretsar, Hamiltonstigar och -cykler

- Sammanhängande grafer, komponenter

[U1.5]

En schematisk karta för labyrinten

Ett exempel på en graf.

En graf

“Teoretisk”, abstrakt

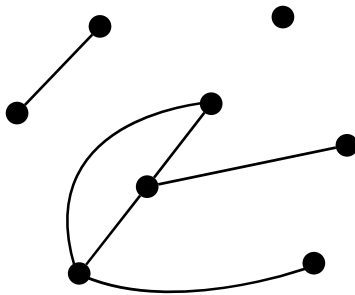
$G = (V, E)$

V — En ändlig mängd, hörn (noder, vertex)
(en. node, vertex (pluralis: vertices)).

E — En mängd av 2-delmängder till V , kanter
(en. edge), (par av olika hörn).

De hörnen är då grannar.

“Praktiskt”

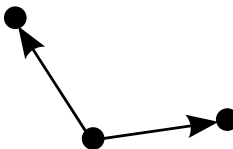


Enkla, oriktade grafer (Behandlas nästan exklusivt i denna kurs.)

Inga:

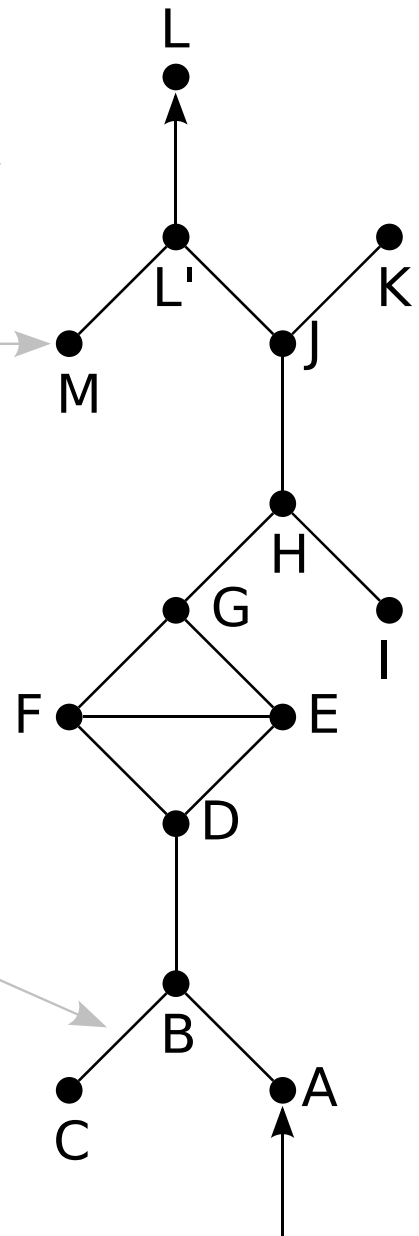


Inte:



hörn, $V \in M$

kant, $E \ni CB$



Varianter av grafer:

Oändlig mängder (hörn)

Riktade kanter

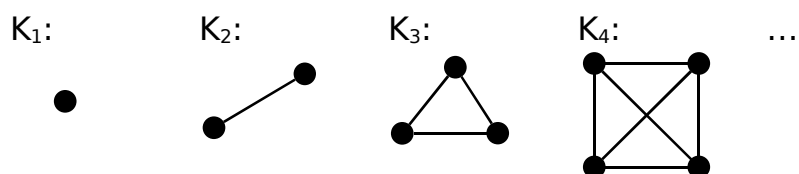
Viktade kanter

Öglor

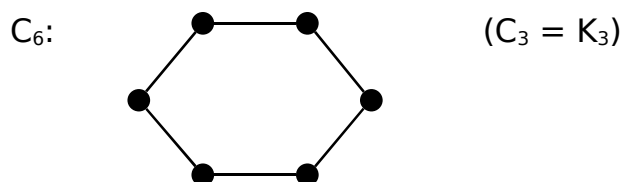
Multipla kanter

Standardnamn för vissa grafer:

K_n , fullständiga grafen med n hörn, $n \geq 1$
Alla möjliga kanter finns.

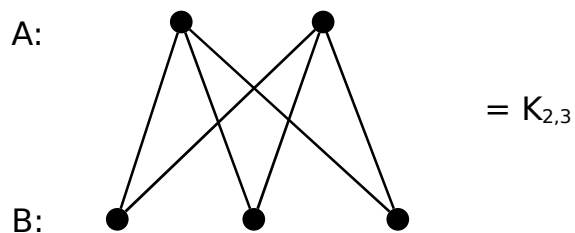


C_n , cykliska grafen med n hörn, $n \geq 3$

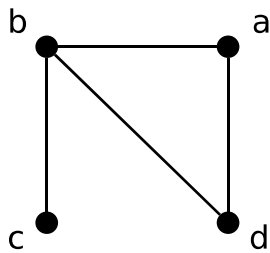


$K_{m,n}$, fullständiga bipartita grafen, $m, n \geq 1$

$V = A \cup B$, A och B disjunkta.



Små grafer ges lätt av en bild, men man kan även använda grannlista (en. adjecant list) eller grannmatris (en. adjecant matrix).



a	b	c	d
b	a	b	a
d	c		b
	d		

	a	b	c	d
a	0	1	0	1
b	1	0	1	1
c	0	1	0	0
d	1	1	0	0

För enkel oriktad: Symmetrisk 0/1-matris, 0:or på diagonalen.

(inga multipla kanter)

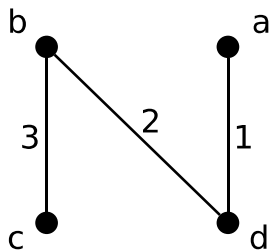
(inga öglor)

(oriktad)

$$G = (V, E)$$

$$a_{ij} = \begin{cases} 1 & \text{om } \{ij\} \in E \\ 0 & \text{annars} \end{cases}$$

Ett sätt till: incidentmatris



	1	2	3
a	1	0	0
b	0	1	1
c	0	0	1
d	1	1	0

Exakt 2 1:or i varje kolonn (ty två hörn per kant).

2011-(04)apr-27: dag 2, 24

Del 2, på denna dag!
Nu föreläsning

Fortsättning om grafer

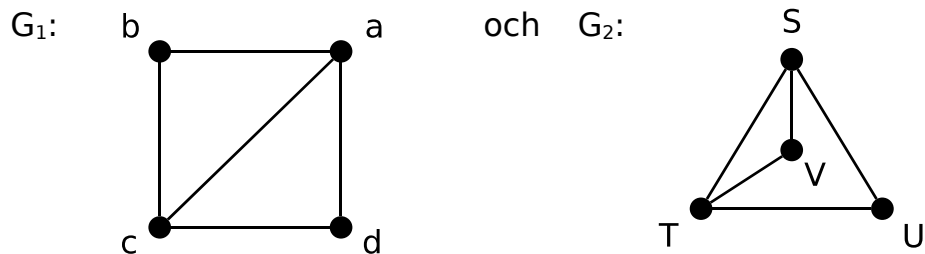
$G = (V, E)$ E — Mängden av kanter (2-delmängder av V)
 V — Mängden av hörn

Isomorfi mellan grafer ("strukturellighet")

$G_1 = (V_1, E_1)$ är isomorfisk med
 $G_2 = (V_2, E_2)$ betyder att det finns en bijektion $\phi : V_1 \rightarrow V_2$ så att

$$\{x, y\} \in E_1 \Leftrightarrow \{\phi(x), \phi(y)\} \in E_2$$

Exempel:



är isomorfa med isomorfi $\phi = \begin{pmatrix} a & b & c & d \\ S & V & T & U \end{pmatrix}$.

Valensen (graden) för ett hörn $v \in V$:

$\delta(v)$ = antalet kanter där v ingår, (öglor räknas dubbelt).

I exemplet:

$$\delta(a) = 3 = \delta(U), \quad \delta(b) = 2$$

En graf är n -reguljär om alla hörn har valens n .

Exempel: K_n är $(n - 1)$ -reguljär.
 C_n är 2-reguljär.

Sats:

$$\sum_{v \in V} \delta(v) = 2|E|$$

Ty: Till varje hörn, v , "hör" $\frac{1}{2} \delta(v)$ kanter så $|E| = \sum_{v \in V} \frac{1}{2} \delta(v)$.

Följdsats:

Antalet udda hörn (det vill säga hörn med udda valens) är jämnt.

Exempel:

En 3-reguljär graf har ett jämnt antal hörn, $|V|$ jämnt och $|E|$ delbart med 3.

$$\left(\sum_{v \in V} \underbrace{\delta(v)}_3 = 3|V| = 2|E| \right)$$

Exempel:

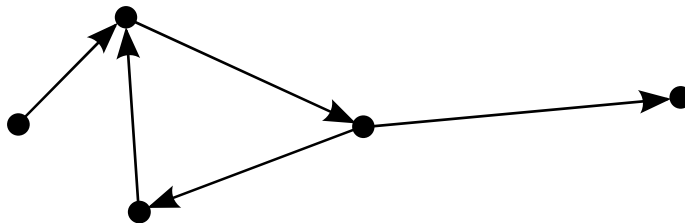
G är 5-reguljär och har 8 hörn, hur många kanter?

$$\sum_{v \in V} \underbrace{\delta(v)}_5 = 5 \underbrace{|V|}_8 = 2|E| \quad \text{så} \quad |E| = 20$$

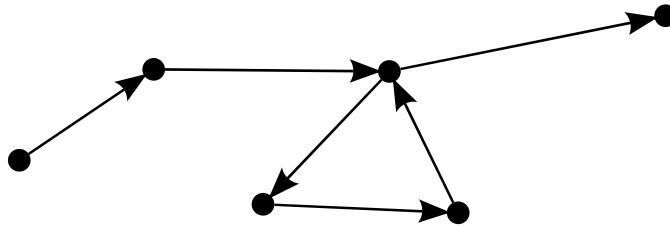
Namn för olika kantföljder i en graf:

Vandring (en. walk)

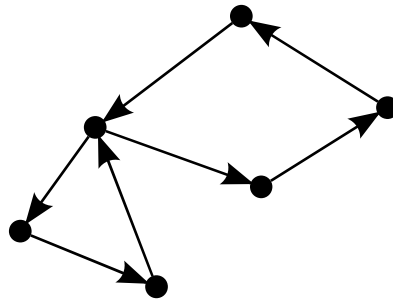
Från hörn till grannhörn. $\{v_i, v_{i+1}\} \in E, v_i \in V$.



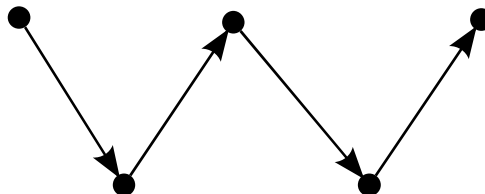
Väg (en. trail) Vandring utan upprepade kanter.



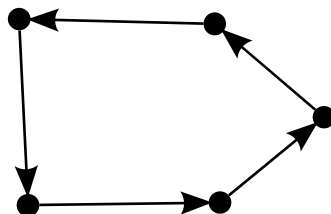
Krets (en. circuit) Sluten väg, $v_1 = v_k$



Stig (en. path) Väg utan upprepade hörn



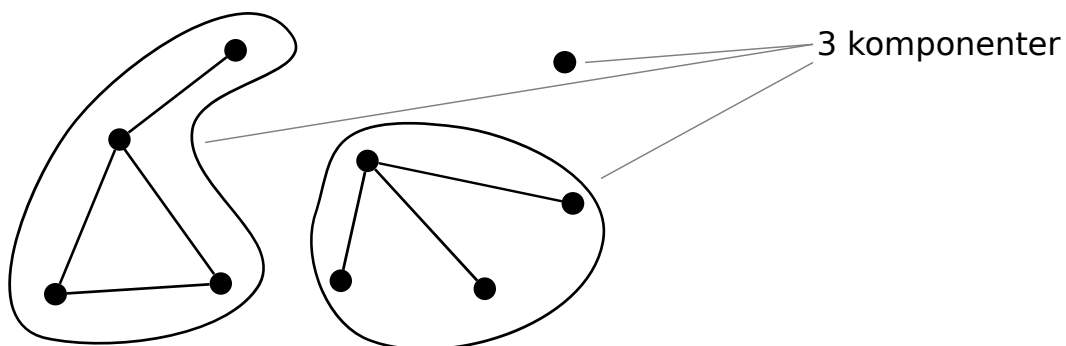
Cykel (en. cycle) Sluten stig



En graf är sammanhängande omm varje par hörn kan förbindas med en vandring, väg eller stig.

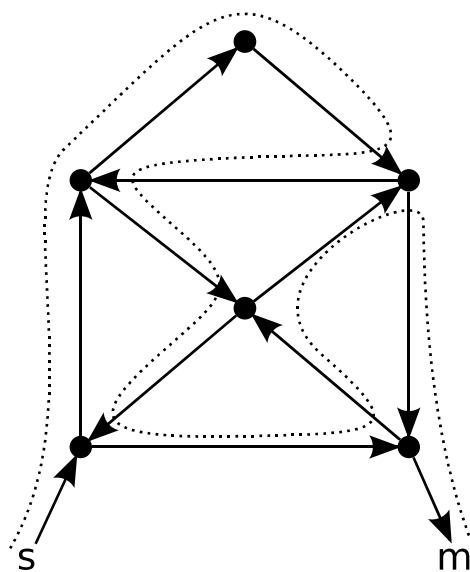
Relationen mellan hörn och att kunna förbindas är en ekvivalensrelation.
Ekvivalens klasser: grafens komponenter

Exempel:



En Eulerväg är en väg som passerar varje kant exakt en gång.

Exempel:



Har en Eulerväg men ingen Eulerkrets.

Sats:
(Euler)

En graf, G , har en Eulerväg om G är sammanhängande och har högst 2 udda hörn.

G har en Eulerkrets om dessutom alla hörn är jämna.

Varför:

Starta i ett udda hörn (om något finns) och vandra längs några kanter så länge det går. Stopp i ett udda hörn (eller där vi startade).

2011-(04)apr-28: dag 3, 25

Del 2 på denna dag!

Mer om grafteori

Resten från övning 8.

Träd

Spännande träd

Minimala spännande träd, Kruskals algoritm

Binära rotade träd

Planära grafer

Eulers polyederformel

K_5 och $K_{3,3}$ är inte planära, Kuratowskis sats

Övnings-KS 4

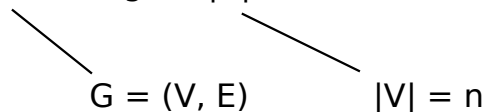
Anmälan till tentan senast 15 maj.

En Hamiltonstig/-cykel passerar varje hörn i grafen precis en gång.

Man kan sätta ihop en Eulerväg/-krets med flera Eulerkretsar.

Försättning av övning 8.

5) G är en graf, $|V| \geq 2$. Visa att två hörn har samma valens.



Möjliga valenser: $0, 1, 2, \dots, n-1$, n stycken olika.

n hörn, men valensen 0 och $n-1$ kan inte förekomma i samma graf.

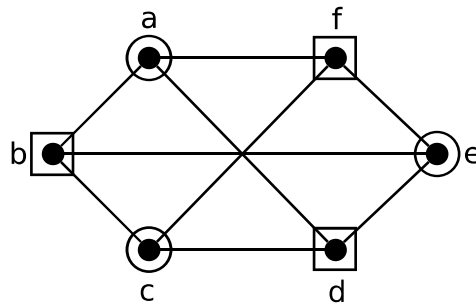
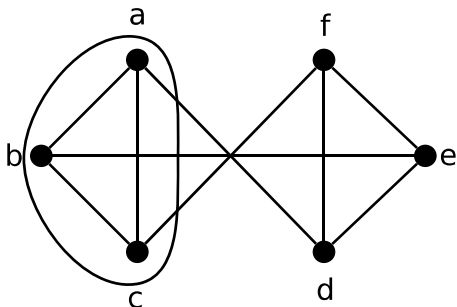
I varje fall $n-1$ möjliga värden, enligt postfacksprincipen har två hörn samma valens.

6) Granntabeller för G_1, G_2 :

a	b	c	d	e	f
b	a	a	a	b	c
c	c	b	e	d	d
d	e	f	f	f	e

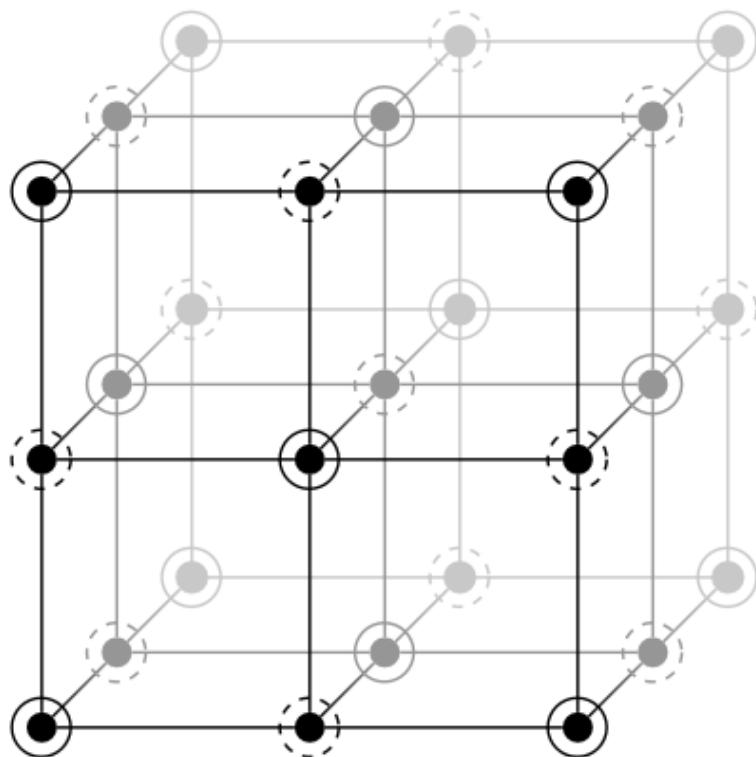
&

1	2	3	4	5	6
2	1	2	3	2	1
4	3	4	5	4	3
6	5	6	1	6	5



G_2 är bipartit; G_1 inte, så de är inte isomorfa.

7)



3×3×3-ost

Musen vill följa en Hamiltonstig i ostgrafen, se figuren ovan.
Vi skall visa att han inte kan sluta i mitten hörnet.
(Hörn faller inte ned, när de förlorar sitt stöd, de svävar.)

Experiment visar att det verkar vara så, men varför?

Grafen är bipartit, se ringarna.

Heldragna: $|X| = 14$

Sträckade: $|Y| = 13$

En Hamiltonstig måste börja och sluta i X-hörn. Mitt hörnet är ett Y-hörn.

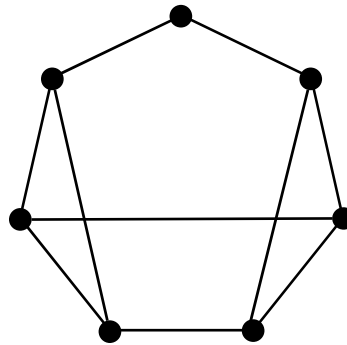
8) Finns (enkla) grafer med 7 hörn med valenserna:

a) 0, 2, 3, 3, 4, 4, 5?

Nej, ty summan av valenserna måste vara $2|E|$, ett jämnt tal.

b) 2, 3, 3, 3, 3, 3, 3?

Ja. Exempel:



c) 2, 2, 3, 5, 5, 5, 6?

Granne med alla. -1 på alla valenser och bort med den.

Ingen sådan graf finns, varje 1-hörn har kant till högst 4-hörn, så ett 4-hörn skall ha högst 3 grannar.

Alternativt:

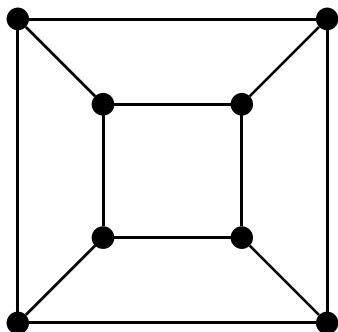
(2, 2, 3) har högst 7 kanter ut,
(5, 5, 5, 6) har minst 9 kanter ut.

Omöjligt.

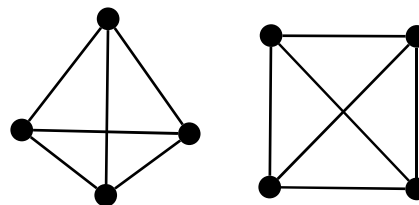
(Finns med öglor.)

9) 3-reguljära grafer med 8-hörn.

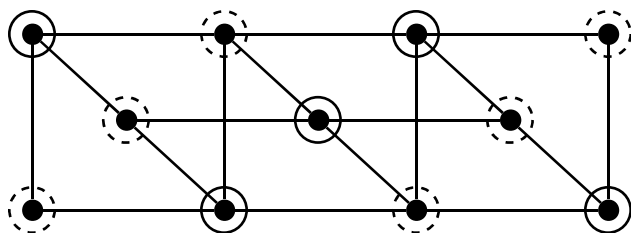
Kubgrafen:



Inte sammanhängande:

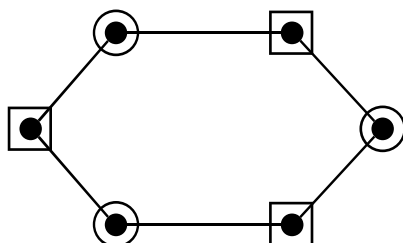


12)



Grafen har ingen Hamiltoncykel ty den är bipartit med $|X| = 6$, $|Y| = 5$.

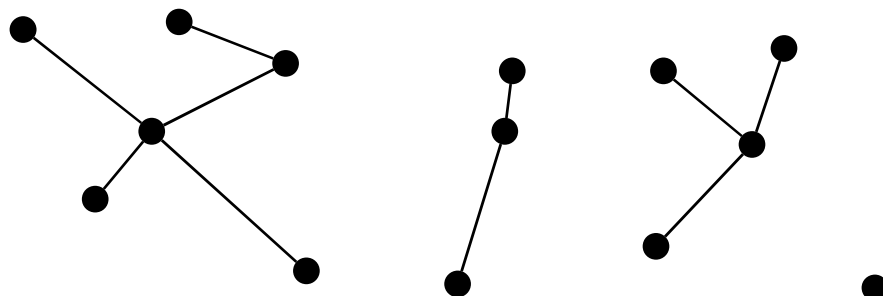
En cykel i en bipartit graf har lika många hörn av varje typ.



2011-(05)maj-03: dag 4, 26

Skog:

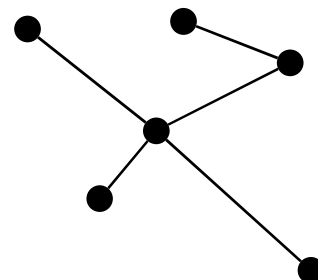
En graf utan cykler kallas "skog"



Varje komponent i en skog kallas träd:

Ett träd är sammanhängande^① och icke-cykliskt^②.

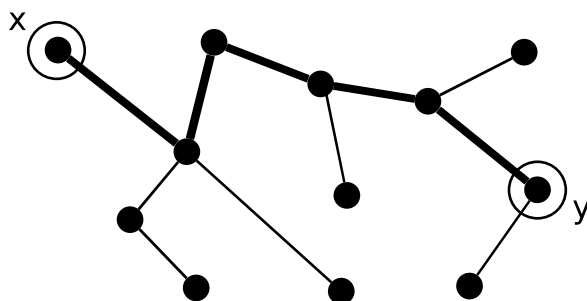
Träd brukar betecknas $T = (V, E)$ (eller $T(V, E)$)



Sats:

Om $T = (V, E)$ är ett träd:

③ För alla $x, y \in V$ finns en unik stig mellan x och y .



④ Om en kant i ett träd toges bort, så delas trädet upp i två träd; grafen har då två komponenter istället för en.

⑤ $|E| = |V| - 1$ (om $V \neq \emptyset$)

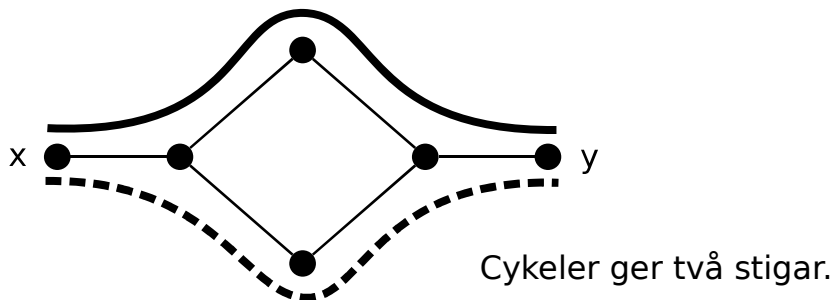
Anledning:

③ Kan används som en alternativ definition av träd.

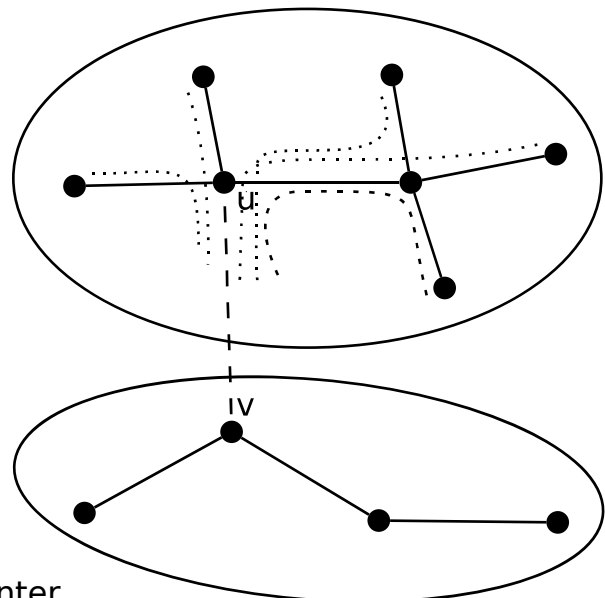
③ \Rightarrow ① Enligt definition av sammanhängande.

③ \Rightarrow ② Ty en cykel skulle ge 2 olika stigar mellan x och y på cykeln.

①, ② \Rightarrow ③ Från x till y finns minst en stig, om det finns två olika stigar så finns det en cykel.



④ Om vi tar bort en godtycklig kant (här $\{uv\}$) så bildas två komponenter (de hörn vars stig till v passerar u, och de som inte gör det). Komponenterna är fortfarande träd eftersom ingen cykel har bildas.



⑤ Visas med induktion över $|E|$

Bas: Om $|E| = 0$, $|V| = 1$
(en hörn och ingenting mer) OK!

Steg: Antag sant för träd med färre kanter än $|E|$.

Tag bort en kant i $T = (V, E)$, då får man $T_1 = (V_1, E_1)$ och $T_2 = (V_2, E_2)$ enligt ④.

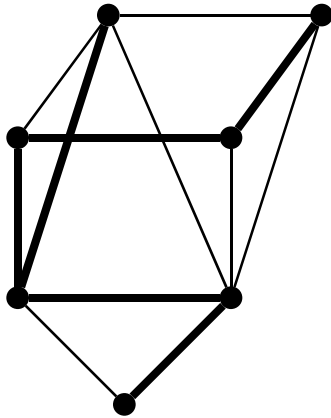
$$|E| = |E_1| + |E_2| + 1 = \{\text{induktions antagande}\} = |V_1| - 1 + |V_2| - 1 + 1 = |V_1| + |V_2| - 1 = |V| - 1$$

■

Varje sammanhängande graf har minst ett (upp)spännande träd.
Det vill säga ett träd som innehåller en del av kanterna.

$$T = (V, E'), \quad E' \subseteq E$$

Exempel (G är smalt och tjockt, T är tjockt):



Tag bort en kant i en graf så länge det går.

— eller —

Starta utan kanter och lägg till kanter så länge det går utan att det bildas cykler.

För en viktad sammanhängande graf (kant e har vikten $\omega(e)$) kan man finna ett minimalt spännande träd, ett spännande träd med minimal viktsumma, med Kruskals algoritm.

Kruskals algoritm:

Lägg i vaje steg till den lättaste kanten som inte ger någon cykel med de redan valda.

Kruskals algoritm är en girig algoritm, det vill säga att den optimerar varje steg istället för att göra Brute Force (testa alla existerande varianter) eller planera i förväg.

Bevis:

Algoritmen ger ett spännande träd, T , med kanter, valda i ordningen e_1, e_2, \dots . Om T inte är minimalt, låt T_1 vara ett minimalt spännande träd med så många e_1, e_2, \dots, e_{k-1} gemensamma med T_1 men inte e_k .

Om e_k läggs till T_1 fås en cykel med något e'_k som inte ligger i T .
 $\omega(e'_k) \geq \omega(e_k)$ såsom T bildades, annars hade vi ju valt e'_k (såsom T valdes).

Om vi i T_1 ersätter e'_k med e_k så får vi ett träd T_2 med vikt $\leq T_1$ och en kant mer gemensam med T .

Det vill säga T_2 's vikt = T_1 's eftersom T_1 hade minimal vikt.

Motsäger valet av T_1 , så $T_1 = T$.

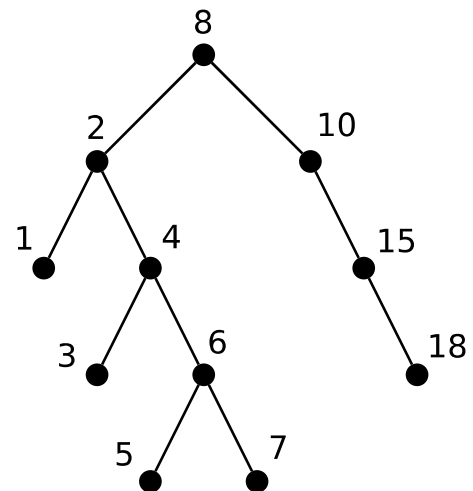
Binära rotade träd

Viktiga för sortering.

Ett träd har ett hörn som utsetts till rot, varje hörn har högst två barn. Ett barn är grannar som inte leder mot roten. Grannar som leder mot roten kallas förfädrar, den första av dem kallas förälder.

Typisk användning:

Lagring och sökning av ordnad data.



Element vid ett hörn:

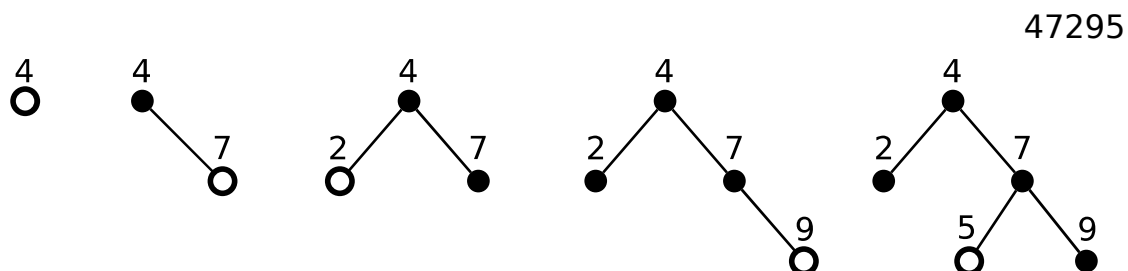
Större än alla till vänster, mindre än alla till höger.

Ett lagringsträd skapas lätt rekursivt:

Om trädet är tomt:
annars:

skapa rot för trädet
talet > rot lägg till höger
talet < rot lägg till vänster

(något förenklat!)

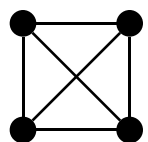


Planära grafer

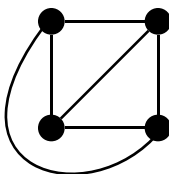
Om en graf är ritad i ett plan *eller på en sfär* utan att några kanter korsar, så kallas grafen plan

En planär graf är en graf som är isomorf med någon plan graf.

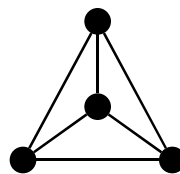
Exempel på isomorfa planära grafer (K_4):



inte plan

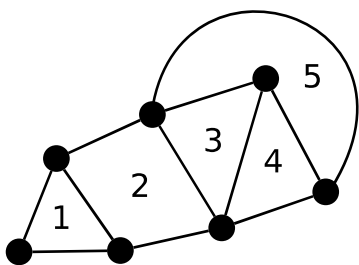


plan

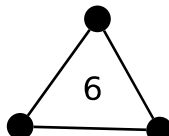


plan

En plan graf definierar områden i planet. Vi kallar dem ytor (fasetter i boken).
Om den plana grafen är ritad i ett plan fås en obegränsad yta.



7



$v = 10$ — hörn
 $e = 14$ — kanter
 $r = 7$ — ytor
 $c = 2$ — komponenter

Sats:

För en plan graf med v hörn, e kanter, r ytor och c komponenter gäller:

$$v - e + r - c = 1 \quad (\text{mnemonik: verk!, naturligtvis med !})$$

Om grafen är sammanhängande ($c = 1$):

Eulers polyederformel:

$$v - e + r = 2$$

Bevis:

Induktion över e .

Bas:

Om $e = 0$; $c = v$, $r = 1$ OK!

Steg:

Antag att påståendet stämmer med $e = k$.

Låt G ha $e = k + 1$.

Tag bort en kant från G , få G' .

Två fall:

- 1) Samma yta på båda sidor om borttagna kanten.

Då har G' fler komponenter än G .

$$\begin{array}{ll} v' = v & e' = e - 1 = k \\ r' = r & c' = c + 1 \end{array}$$

Så:

$$\begin{aligned} v' - e' + r' - c' &= v - (e - 1) + r - (c + 1) = \\ &= \{\text{induktions antagande}\} = v - e + r - c \end{aligned}$$

- 2) Olika ytor jämte borttagna kanten.

$$\begin{array}{ll} v' = v & e' = e - 1 \\ r' = r - 1 & c' = c \end{array}$$

Så:

$$\begin{aligned} v' - e' + r' - c' &= v - (e - 1) + (r - 1) - c = \\ &= v - (e - 1) + r - (c + 1) = \text{som i fall 1.} \end{aligned}$$

Satsen ger nödvändiga villkor för planaritet:

Om G , sammanhängande, är enkel (inga ölgor eller multipla kanter), så begränsas varje uta av minst tre kanter (om $e \geq 2$!).

$$\text{Så: } 2e = \sum_{\text{områden}} \underbrace{(\text{antalet kanter kring området})}_{\geq 3} \geq 3r$$

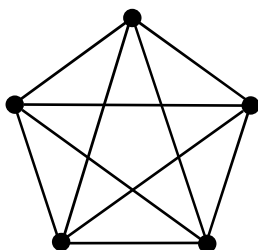
$$\text{Så: } e \geq \frac{3}{2}r \quad r \leq \frac{2}{3}e \quad \Rightarrow \quad e = v - e + r \leq v - \frac{1}{3}e$$

$$3v \geq e + 6$$

Så K_5 är ej planär!

$$v = 5, \quad e = 10$$

$$15 \not\geq 16$$




2011-(05)maj-04: dag 5, 27

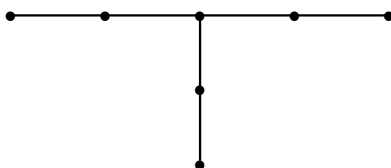
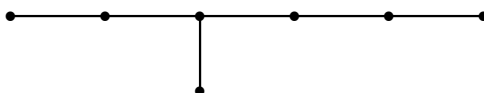
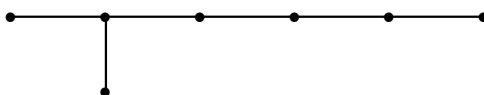
Övning 9

- 1) Rita alla (icke-isomorfa) träd (sammanhängande, acyklisk graf) med 7 hörn. En av varje isomorfityp.

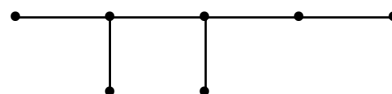
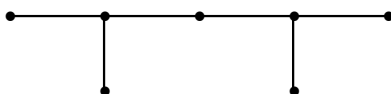
Max valens:

2: 

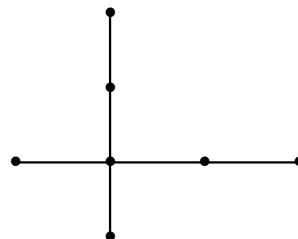
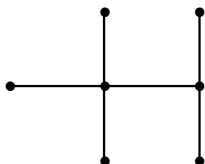
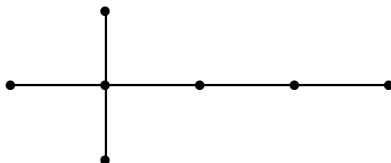
3: 1) 1 hörn med valens 3:



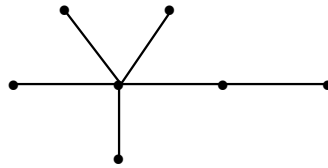
2) 2 hörn med valens 3:



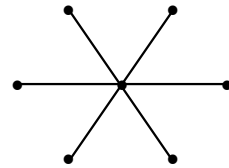
4:



5:



6:



Totalt 11 olika.

- 2) Grafen $G = (V, E)$ saknar cykler, $|V| = 143$, $|E| = 100$.
Hur många komponenter?

(G är en skog.) Varje komponent är ett träd (sammanhängande och acyklisk), så antalet hörn i den är 1 mer än kanter, i den [trädet].
 k stycken komponenter ger alltså $143 - 100 = 43$ komponenter.

- 3) $G = (V, E)$ med $\delta(x) + \delta(y) \geq n + 1$, ($n = |V|$), alla, $x, y \in V$.
Vi skall visa att G är sammanhängande.

Motsägelsevis:

Antag att G inte är sammanhängande, $V = V_1 \cup V_2$, $V_1 \cap V_2 = \emptyset$,
och inga kanter mellan $u \in V_1$ och $v \in V_2$.

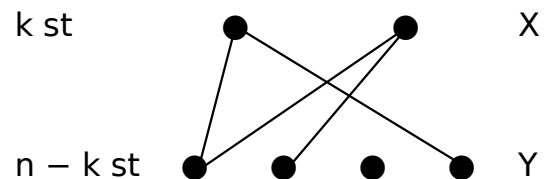
Om $x \in V_1 : \delta(x) \leq |V_1| - 1$
 $y \in V_2 : \delta(y) \leq |V_2| - 1$

då $\delta(x) + \delta(y) \leq |V_1| + |V_2| - 2 = n - 2$.
Motsägelse!

- 4) $G = (V, E)$ bipartit ($V = X \sqcup Y$) (\sqcup används inte av läraren;
 $V = X \sqcup Y$ betyder $V = X \cup Y$, $X \cap Y = \emptyset$.)

$|V| = n$, låt $|X| = k$, $|Y| = n - k$

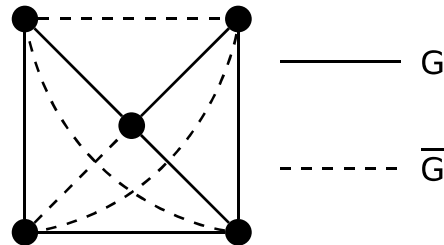
$$\begin{aligned} \text{Då: } e = |E| &= \sum_{x \in X} \underbrace{\delta(x)}_{\leq n-k} \leq k(n-k) = \\ &= \left(\frac{n}{2}\right)^2 - \left(k - \frac{n}{2}\right)^2 \leq \left(\frac{n}{2}\right)^2 \end{aligned}$$



- 5) Till grafen $G = (V, E)$ bildas dess komplementgraf $\bar{G} = (V, E')$ så att $E \cap E' = \emptyset$, $K_n \cong (V, E \cup E')$, ($|V| = n$),

isomorfsk med (skrivs ibland \cong , \approx)

det vill säga; det går kanter i \bar{G} mellan hörn x och y om det inte går en kant mellan dem i G .



Om ett hörn har valens δ i G , har det valens $(n - 1) - \delta$ i \bar{G} .

- a) Valenssekvensen $\delta_1, \delta_2, \dots, \delta_n$ ger valenssekvensen i \bar{G} :

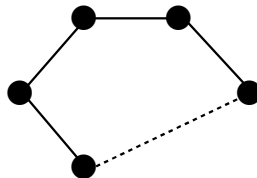
$$n - 1 - \delta_1, \dots, n - 1 - \delta_n$$

- b) Om G är k -reguljär (det vill säga $\delta_1 = \delta_2 = \dots = \delta_n = k$
 (kan skrivas $\delta \cong k$, notera spegelvänt tilde))
 är \bar{G} således $(n - 1 - k)$ -reguljär.

Så enda möjliga \bar{G} :

$$C_8, C_5 + C_3, C_4 + C_4$$

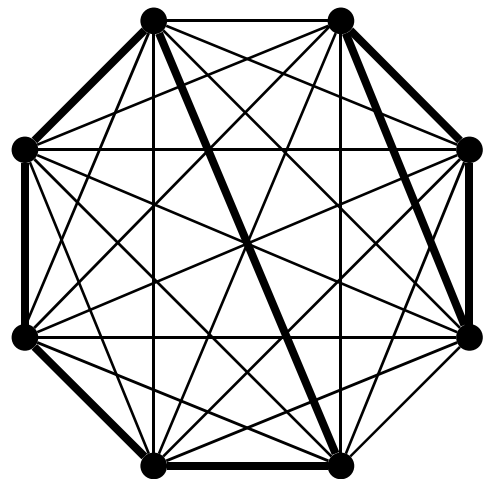
$$C_n, n \geq 3$$



Till exempel G som svarar mot
 $\bar{G} = C_5 + C_3$:

\bar{G} tjock

G smal

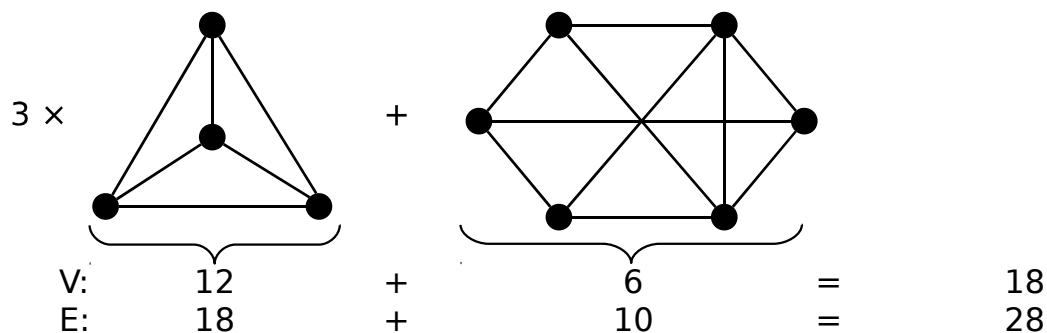


- 7) $G = (V, E)$, $\delta(v) \geq 3$ för alla $v \in V$, $|E| = 28$
Hur stort kan $|V|$ vara?

$$\underbrace{\sum_{v \in V} \delta(v)}_{\geq 3|V|} = 2|E|, \text{ så } |V| \leq \frac{2 \cdot 28}{3} = 18 \frac{2}{3}$$

Alltså $|V| \leq 18$.

Men finns en sådan?



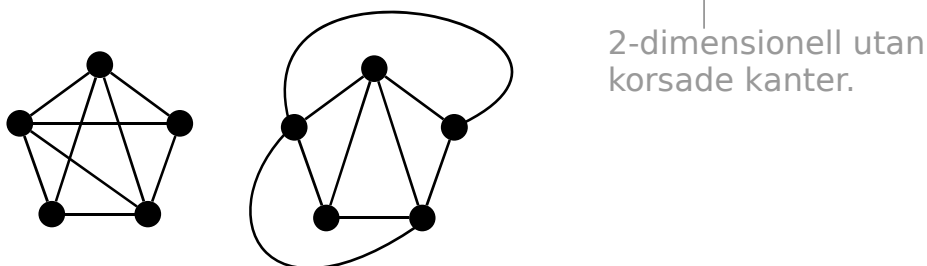
Så ja, $|V| = 18$ är möjligt.

- 8) Visa G osammanhängande $\Rightarrow \overline{G}$ sammanhängande.

x, y inte grannar i G : xy en väg mellan dem i \overline{G} .

x, y grannar i G , z i en annan komponent: xzy en väg i \overline{G} .

- 9) $(K_5 - 1 \text{ kant})$ är planär: (planär = kan ritas som en plan graf.)



10) $G = (V, E)$ sammanhängande, 4-reguljär och planär, $e = |E| = 16$.

Vad är r , antalet ytor för en plan ritning av G ?

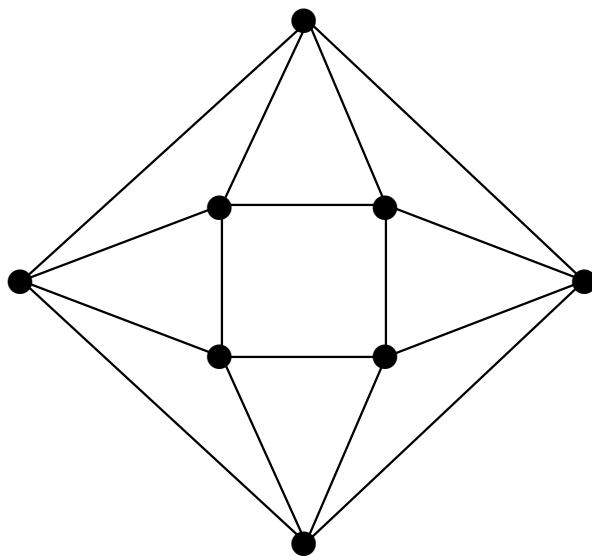
Eulers polyederformel för sammanhängande grafer:

$$v - e + r = 2 \quad (r \text{ kallas ibland f.})$$

$$4v = \sum_{x \in V} \delta(x) = 2e = 32 \quad \text{så } v = 8 \text{ och}$$

$$r = 2 - v + e = 2 - 8 + 16 = 10$$

Exempel:



11) $G = (V, E)$ sammanhängande planär har ingen cykel av längd $< k$, $k \geq 3$.

$$\text{Då är } k \cdot r \leq \sum \underbrace{\text{antalet kanter kring ytan}}_{\geq k} = 2e$$

$$\text{Så } r \leq \frac{2}{k}e \quad (\text{varje bipartit graf: } k = 4)$$

$$2 = v - e + r \leq v + \underbrace{\left(\frac{2}{k} - 1\right)}_{< 0}e, \quad e \leq \frac{k}{k-2}(v-2)$$

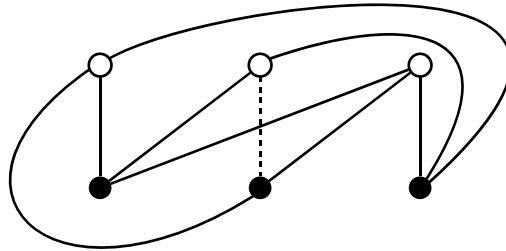
$$K = 3: \quad e \leq 3(v - 2)$$

$$K = 4: \quad e \leq 2(v - 2)$$

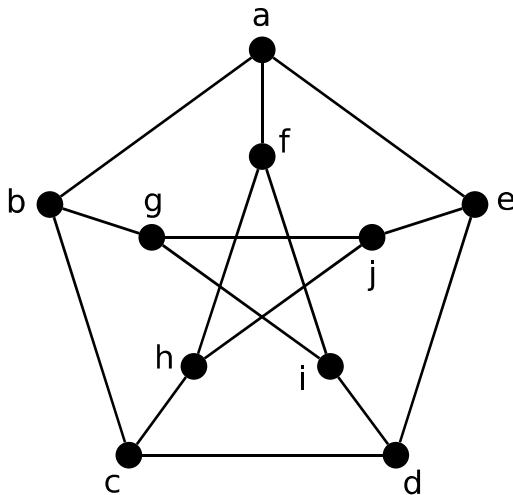
$K_{3,3}$ är inte planär:

$$e = 9, v = 6, 2(v - 2) = 8$$

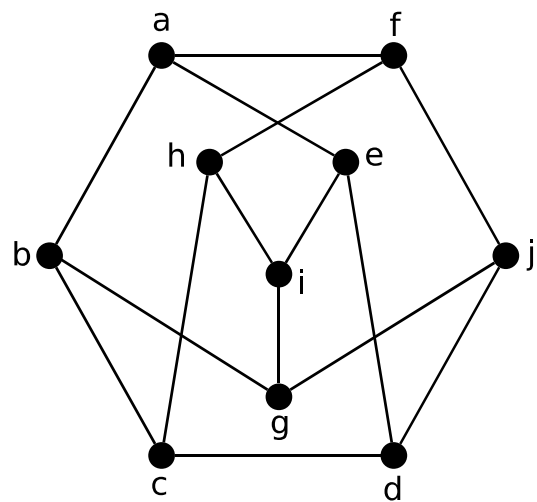
$$e > 2(v - 2) \quad \text{inte planär}$$



Petersens graf:



(Alternativt:)



Petersens graf har inga cykler av längd ≤ 4 , det vill säga $k = 5$ i:

$$e \leq \frac{k}{k \cdot 2}(v - 2) = \frac{5}{3}(v - 2)$$

$$e = 15, v = 10$$

$$\frac{5}{3}(v - 2) = \frac{5}{3}8 = 13\frac{1}{3}$$

Så grafen är inte planär (inte ens om man tar bort ett hörn och dess kanter).

Kuratowskis sats:

Varje icke-planär graf "innehåller" K_5 eller $K_{3,3}$, och vice versa.



det finns en delgraf som är isomorf med en "subdivision" av K_5 eller $K_{3,3}$.



Den graf med extra hörn på kanter.

Wagners sats:

Detsamma med "innehåller" betyder att den har K_5 eller $K_{3,3}$ som minor.
Det vill säga någon kantkontraktion av grafen har K_5 eller $K_{3,3}$ som delgraf.

Bort tagning av hörn i Petersensgraf:

Se: <http://en.wikipedia.org/wiki/File:Kuratowski.gif>

Notera att för satserna ovan gäller 'om och endast om' för hållande och 'inklusive eller' villkor. Inte 'endast om' och 'exklusivt eller' som läraren råkade skriva.

2011-(05)maj-09: dag 6, 28

Mer om grafer

Planära grafer (fortsättning)

“Platonska grafer”

Duala grafer

(Hörn)färgning av grafer

Kromatiska talet, $\chi(G)$

En girig algoritm

Sex-, fem- och fyrfärgssatsen

Kromatiska polynomet, $P_G(\lambda)$

Matchning i grafer

Fullständig och maximal matchning

Bipartita grafer

Halls sats (giftermålssatsen)

Utökande alternerande stigar

Distinkta representater (transversalerna)

Ö9:12)

$G = (V, E)$ sammanhängande, plan

$v = |V| = 12, r = 11$

$\delta(h) = 3$ eller 5 för alla $h \in V$.

Hur många av varje?

Låt antalet hörn med valens 3 vara x .

Antalet med valens 5.

Eulers polyederformel:

$$v - e + r = 12 - e + 11 = 2$$

Så: $e = 21$

$$\sum_{h \in V} \delta(h) = \underbrace{2|E|}_{2e} : 3 \cdot x + 5(12 - x) = 2 \cdot 21$$

ger $x = 9$

“Platonska grafer” (inte standardnamn)

Platonska kroppar (en. *Platonic solids*) (polyedrar, en. *polyhedron[s]*) med alla hörn (n kanter) och alla sidor (regelbundna m -hörningar) kongruenta.

Det finns precis 5 stycken olika.

Animeringar:

<http://en.wikipedia.org/wiki/File:Tetrahedron.gif>

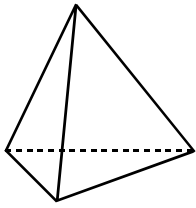
<http://en.wikipedia.org/wiki/File:Hexahedron.gif>

<http://en.wikipedia.org/wiki/File:Octahedron.gif>

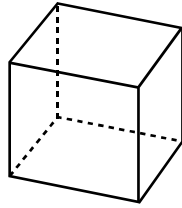
<http://en.wikipedia.org/wiki/File:Dodecahedron.gif>

<http://en.wikipedia.org/wiki/File:Icosahedron.gif>

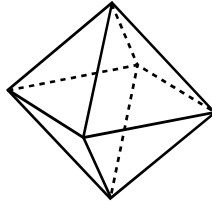
(Bilder på nästa sida.)



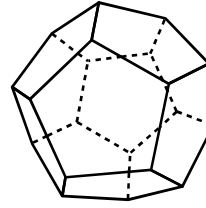
Tetraeder



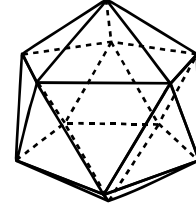
Hexaeder



Oktaeder



Dodekaeder



Ikosaeder

Tetraeder: (en. tetrahedron)

Hexaeder: (en. hexahedron)

Oktaeder: (en. octahedron)

Dodekaeder: (en. dodecahedron)

Ikosaeder: (en. icosahedron)

Tresidig pyramid

Kub

Dubbel fyrsidig pyramid; T8- (D8) tärning

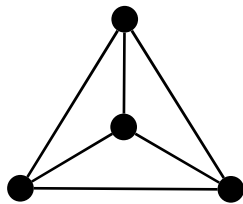
T12- (D12) tärning

T20- (D20) tärning

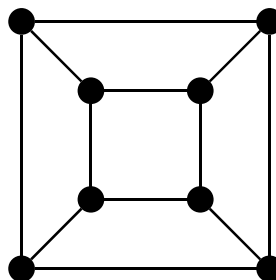
Planar ritningar:

(Kan konstrueras genom att dra ut ena sidan så att resten får plats innanför.)

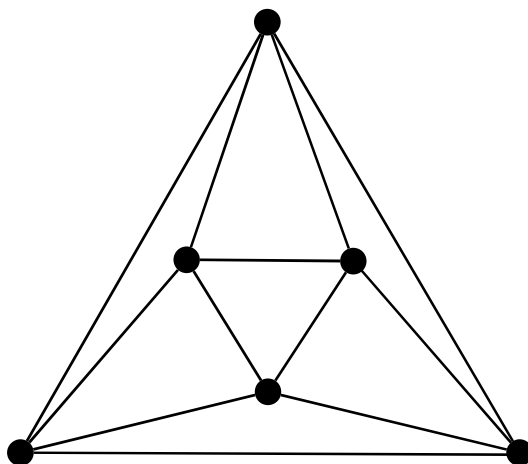
Tetraeder



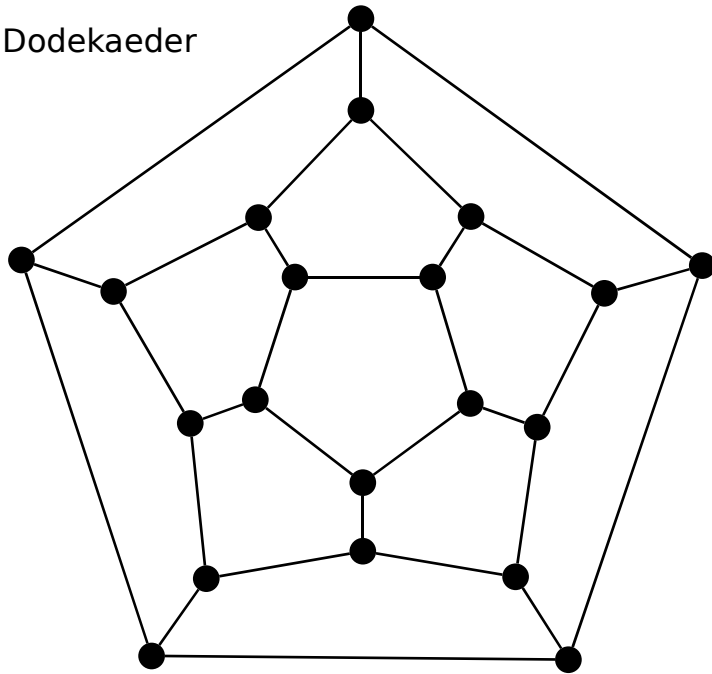
Hexaeder



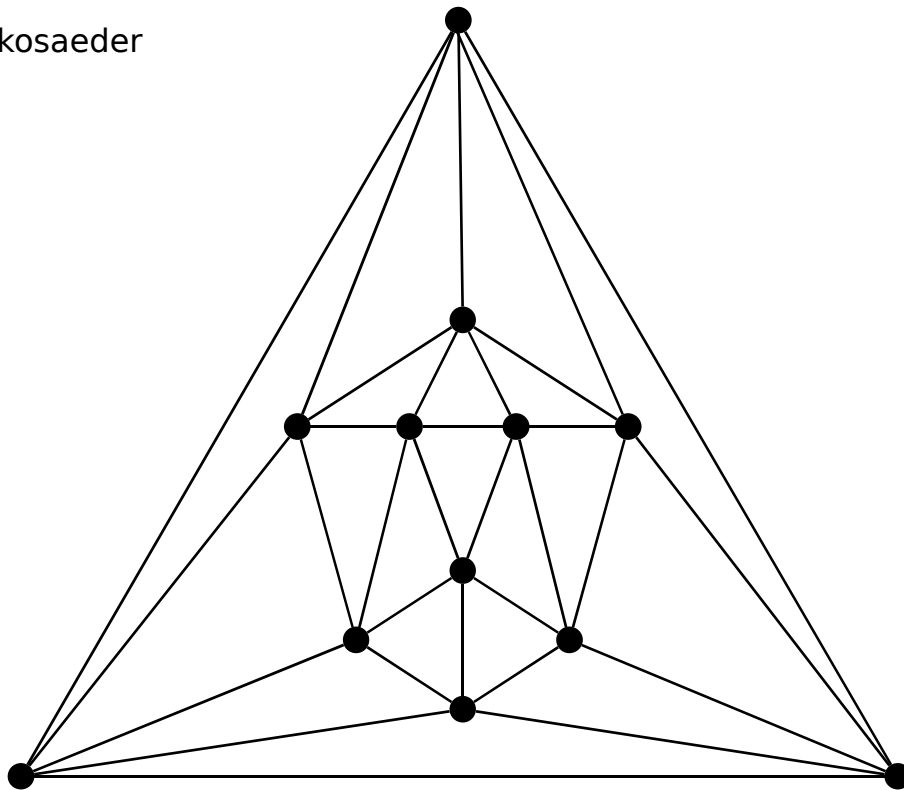
Oktaeder



Dodekaeder



Ikosaeder



En "dubbelt reguljär" graf: sammanhängande, plan med samma valens ($n \geq 3$) i alla hörn, samma antal ($m \geq 3$) kanter kring varje yta.

Vi skall se att det bara finns 5 stycken olika:

$$\begin{cases} v - e + r = 2 & (\text{plan, sammanhängande graf}) \\ nv = 2e = mr \end{cases}$$

$$nv = \sum_{x \in X} \delta(x)$$

Så $\frac{2}{n}e - e + \frac{2}{m}e = 2 = \underbrace{(2m - mn + 2n)}_{\text{så: } >0} \frac{e}{mn}$

Det vill säga

$$\begin{cases} (m - 2)(n - 2) < 4 \\ m, n \geq 3 \end{cases}$$

Möjliga m, n :

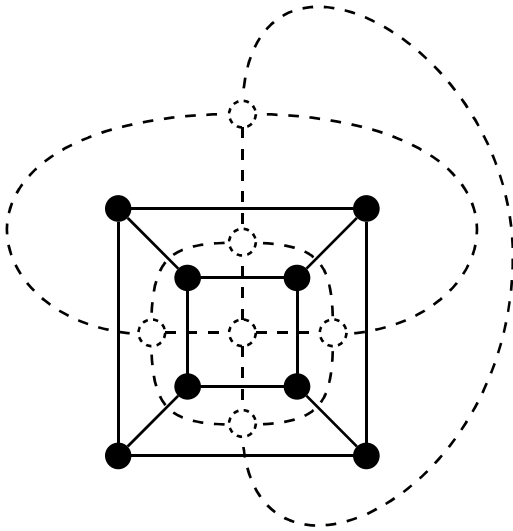
m	n	ger	v	e	r
3	3		4	6	4
• 3	4		6	12	8
– 3	5		12	30	20
• 4	3		8	12	6
– 5	3		20	30	12

• är dualla med varandra
samma sak för –.
($v' = r, r' = v, m' = n, n' = m,$
 $e = e'$ ger dualitet.)

Motsvarande kroppar:

tetraeder
okta-
ikosa-
hexa- (kub)
dodeka-

Den duala grafen G^\perp till en plan graf G beskriver grannrelationen för ytorna i G .



Hörnen i G^\perp svarar mot ytorna i G , en kant i G^\perp mot varje kant mellan ytorna.

Den duala grafen kan ha öglor, multipla kanter.

Heldraget:	G	hexaeder
Halvdraget:	G^\perp	oktaeder

$$(G^\perp)^\perp \cong G$$

(Hörn)färgning av grafer

(Vi kommer inte gå in på kantfärgning.)

$c : V \rightarrow \mathbb{N}$ sådant att
 $\{x, y\} \in E \Rightarrow c(x) \neq c(y)$

Exempel: Schemaläggning av sju föreläsning,
 vissa kan inte ligga samtidigt.

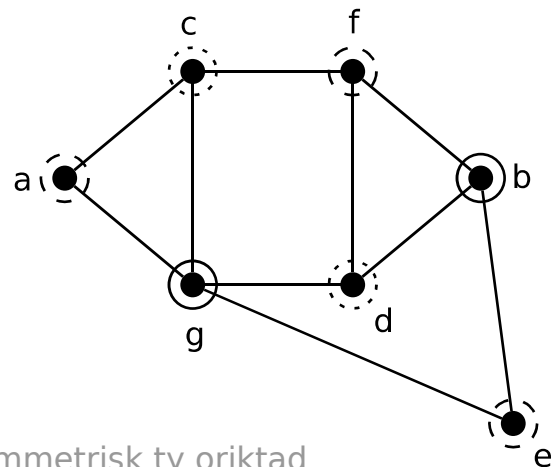
I tabellen på nästa sida markerar 'x' att
 två föreläsningar inte kan ligga samtidigt.

Tabellen uttrycks sedan med en färgad graf.

	a	b	c	d	e	f	g
a			x				x
b				x	x	x	
c	x					x	x
d		x				x	x
e		x					x
f		x	x	x			
g	x		x	x	x		

symmetri

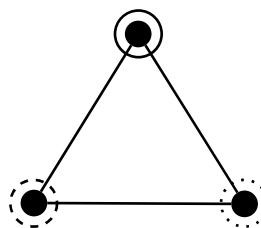
Symmetrisk ty oriktad



Minsta möjliga antalet färger: 3

Möjligt enligt figuren, minsta ty:

En triangel (C_3) kräver 3 färger:



Det kromatiska talet, $\chi(G)$ för G :

Minsta antalet färger som räcker för en hörnfärgning av G .

Exempel:

$$\chi(G) \leq |V|$$

$$\chi(G) = |V| \Leftrightarrow G = K_n, \text{ något } n.$$

$$\chi(G) = 2 \Leftrightarrow \text{Bipartit, } |E| \geq 1$$

$$\chi(G) = 1 \Leftrightarrow |E| = 0, |V| \geq 1$$

$$\chi(G) = 0 \Leftrightarrow |V| = 0$$

Observera att $\chi(G) = k$ betyder:

$$\begin{cases} k \text{ färger räcker} \\ k - 1 \text{ färger räcker inte} \end{cases}$$

I allmänhet svårt att bestämma $\chi(G)$.

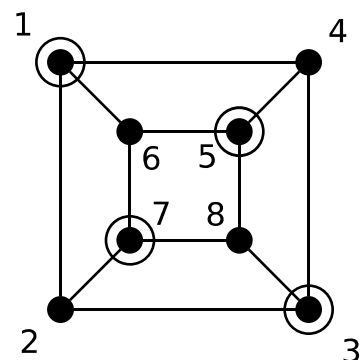
En girig algoritm (ger ofta ganska bra värden):

- 1) Ordna V : v_1, v_2, \dots, v_n $n = |V|$
- 2) Välj i tur och ordning $c(v_1) = 1, c(v_2), c(v_3), \dots$
minsta tillåtna värde (med hänsyn till redan färgade grannar).

Ö9:14)

Ordna hörnen i kubgrafen så att giriga algoritmen ger 2, 3, 4 färger.

2:	v:	1, 2, 3, 4, 5, 6, 7, 8	index
	c:	1 <u>2</u> 1 2 1 2 1 2	färg
3:	v:	1, 8, 2, 3, 4, 5, 6, 7	index
	c:	1 1 2 <u>3</u> 2 3 2 3	färg
4:	v:	1, 8, 5, 2, 3, 4, 5, 6	index
	c:	1 1 2 2 3 <u>4</u> 3 4	färg



Sats: Om G har maxvalens k :

- I) $\chi(G) \leq k + 1$
- II) G sammanhängande och inte reguljär: $\chi(G) \leq k$

Ty:

- I) Klart.
- II) Ordna hörnen $\delta(v_n) < k$, v_{n-1} granne med v_n , v_{n-2} granne med v_{n-1} eller v_n, \dots (går ty G sammanhängande).

Giriga algoritmen ger en färgning med högst k färger, ty varje v har högst $k - 1$ färgade grannar när den färgas.

Exempel:

För en planär graf ($c \geq 1$)

$$\left\{ \begin{array}{l} 3r \leq 2e \\ \updownarrow \\ r \leq \frac{2}{3}e \end{array} \right\} \quad 1 = v - e + r - c \leq v - \frac{1}{3}e - c$$

$$\text{Så } 6v \geq 2e + 6(c + 1) \geq \left(\sum_{x \in X} \delta(x) \right) + k$$

$$\text{Det vill säga: } \left(\sum_{x \in X} \delta(x) - 6 \right) \leq 12$$

Så något hörn har valens ≤ 5 .

6-färgssatsen:

Om G är planär gäller $\chi(G) \leq 6$

Ty:

Induktion över v , antalet hörn.

Bas: $v = 1$ OK

Steg:

Antag att påståendet är sant då $v = k$.

Låt G vara planär med $k + 1$ hörn.

Tag bort ett hörn med valens ≤ 5 (enligt nyss),
får G' . G' färgas med högst 6 färger.

(*)

Sista hörnet (5 grannar av de 6 färgerna) med någon kan färgas.

5-färgssatsen:

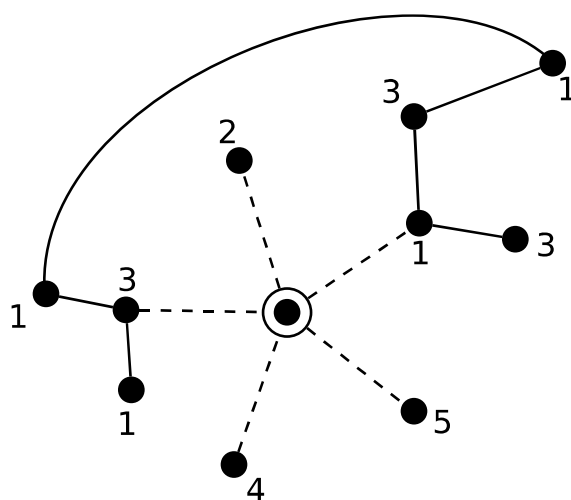
Lite svårare; med samma förutsättningar som i 6-färgssatsen.

Bevis som nyss, fram till (*) i steget.

Om alla grannar (till sista hörnet):

inte olika: Klart.

olika: Bilda 1-3-kedjor.



Om 1-hörnet förbundet med 3-hörnet
finns ingen 2-4-kedja från 2-hörnet till
4-hörnet.

“Byt färger” så något 4 färger på grannarna.

2011-(05)maj-11: dag 7, 29

Mer om grafer

Fortsättning på (hörn)färgning av grafer

Kromatiska polynomet, $P_G(\lambda)$

Matchning i grafer

Fullständig och maximal matchning

Bipartita grafer

Halls sats (giftermålssatsen)

Utökande alternerande stigar

Maximal matchning i bipartita grafer

Distinkta representater (transversalerna)

Övnings-KS 5

Tentaanmälan senast söndag.

Om kromatiska polynomet för en graf $G = (V, E)$:

$P_G(\lambda)$ — antalet sätt att hörnfärga grafen G med λ färger.

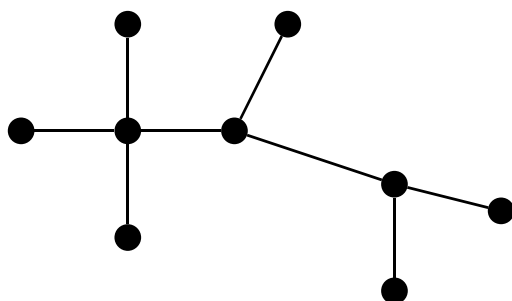
Exempel:

G ett träd $T = (V, E)$

$$P_T(\lambda) = \lambda(\lambda - 1)^{n-1}, \quad |V| = n$$

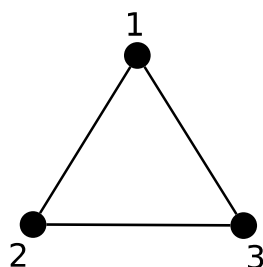
första hörnet

de andra (bara en granne bland resten färgade, ty inga cykler).



Exempel: C_3 :

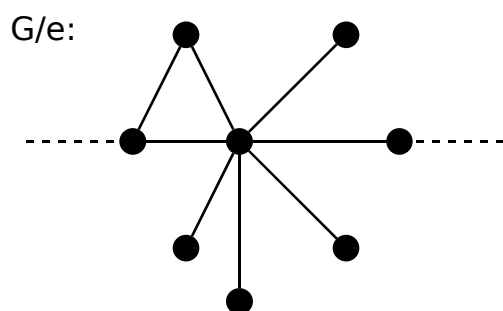
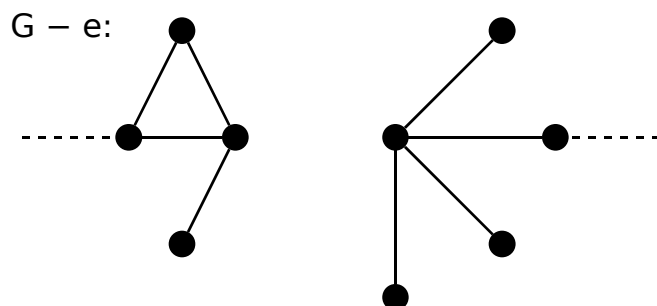
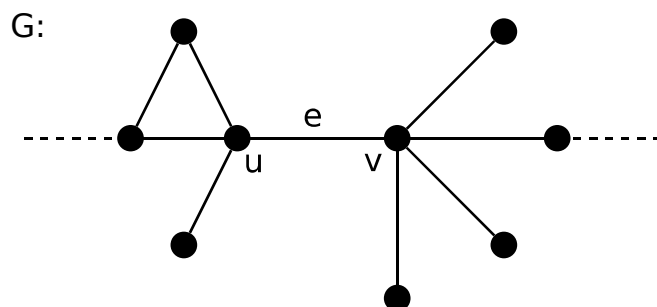
$$P_{C_3}(\lambda) = \lambda(\lambda - 1)(\lambda - 2)$$



Rekursion för att finna $P_G(\lambda)$:

Låt $e \in E$ i $G = (V, E)$

Låt $G - e$: G med e borttagen
 G/e : G med e kontraherad



Då $P_{G-e}(\lambda) = P_G(\lambda) + P_{G/e}(\lambda)$ (additionsprincipen)

\nearrow
 u, v olika färg.

\nearrow
 u, v samma färg.

Så

$$\begin{cases} P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda) \\ P_{(V, \emptyset)}(\lambda) = \lambda^{|V|} \end{cases}$$

ger en rekursion över antalet kanter i grafen.

Med induktion (över antalet kanter) kan då visas:

$$\begin{cases} P_G(\lambda) \text{ är ett polynom i } \lambda. \\ \text{höstgradstermen: } \lambda^{|V|} \\ \text{nästgradstermen: } -|E|\lambda^{|V|-1} \\ \text{koefficienterna är heltal, alternerande } \geq 0, \leq 0. \end{cases}$$

$\chi(G)$: det minsta $\lambda = 0, 1, 2, \dots$ så att $P_G(\lambda) \neq 0$.

Exempel:

$$\begin{aligned} P_{C_n}(\lambda) &= P_{T_n}(\lambda) - P_{C_{n-1}}(\lambda) = \\ &\quad \text{Linjärt träd} \\ &= \underbrace{\lambda(\lambda-1)^{n-1}}_{\lambda-1+1} - P_{C_{n-1}}(\lambda) = \\ &= (\lambda-1)^n + (\lambda-1)^{n-1} - P_{C_{n-1}}(\lambda) \end{aligned}$$

Det vill säga

$$\begin{aligned} P_{C_n}(\lambda) - (\lambda-1)^n &= -(P_{C_{n-1}}(\lambda) - (\lambda-1)^{n-1}) = \\ &= (-1)^{n-3}(P_{C_n}(\lambda) - (\lambda-1)^3) = \\ &= (-1)^{n-3}(\lambda(\lambda-1)(\lambda-2) - (\lambda-1)^3) = \\ &= (-1)^n(\lambda-1) \end{aligned}$$

Så:

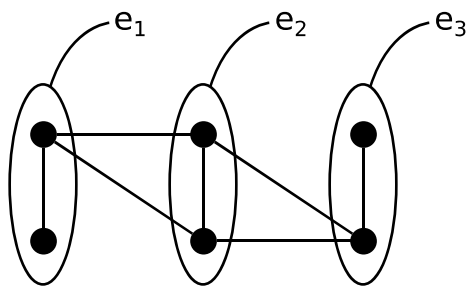
$$P_{C_n}(\lambda) = (\lambda - 1)^n + (-1)^n(\lambda - 1)$$

$$P_{C_n}(0) = 0 = P_{C_n}1$$

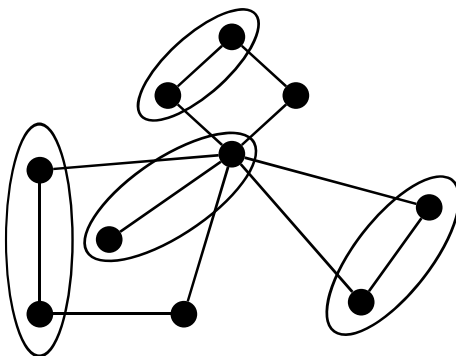
$$P_{C_n}(2) = 1^n + (-1)^n \cdot 1^n = 1 + (-1)^n = \begin{cases} 2 & n \text{ jämnt} \\ 0 & n \text{ udda} \end{cases}$$

Matchning i grafen $G = (V, E)$

en delmängd M till E ($M \subseteq E$) med parvis disjunkta kanter ($\delta(v) \leq 1$).



Fullständig matchning, alla hörn ingår i en kant $M = \{e_1, e_2, e_3\}$.



Maximal matchning
 $|M|$ maximal

Vi talar här om matchning i bipartita grafer, $G = (X \sqcup Y, E)$.

För dem kallar vi en matchning fullständig om $|M| = |X| \leq |Y|$.

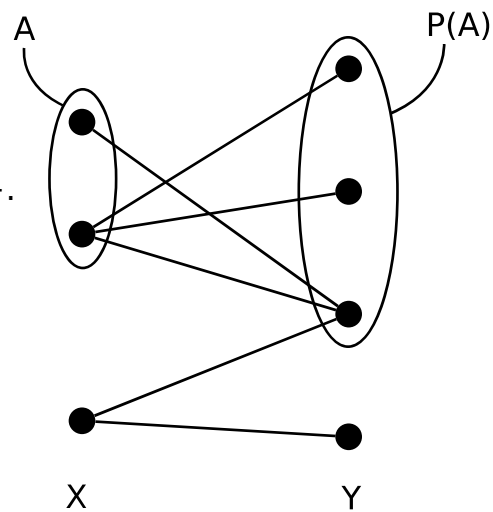
Halls sats: (giftermålssatsen)

En bipartit graf $G = (X \sqcup Y, E)$ har en fullständig matchning omm

$$|P(A)| \geq |A| \text{ för alla } A \subseteq X$$

där

$$P(A) = \{y \in Y \mid \{x, y\} \in E, \text{ något } x \in A\}.$$



Bevis för Halls sats:


- \Rightarrow : Klart
($P(A)$ innehåller alla som de i A matchas med).
- \Leftarrow : Det räcker att visa att (om villkoret är uppfyllt) om en matchning M har $m = |M| < |X|$, finns en matchning M' med $|M'| = m + 1$.

Vi skall finna en utökande alternerande stig i G .

Låt $x_0 \in X$ vara omatchat (i M).

$|P(\{x_0\})| \geq |\{x_0\}| = 1$, så det finns en kant till $x_0 y_1$, i M annars $x_1 y_1 \in M$, $x_1 \neq x_0$. $|P(\{x_0, x_1\})| \geq |\{x_0, x_1\}| = 2$ så det finns $y_2 \neq y_1$, så att $x_0 y_2 \in E$ eller $x_1 y_2 \in E$ och $\notin M$.

Man finner olika y_1, y_2, \dots med en alternerande stig x_0, \dots, y_i .


 varannan kant i M , varannan inte.

Tar slut med att något y_n är omatchat.

Byt matchat-omatchat i stigen x_0, \dots, y_n !
Ger M' med $|M'| = m + 1$.

Sats:

En maximal matchning M av en bipartit graf har storlek $|M| = |X| - \delta(G)$

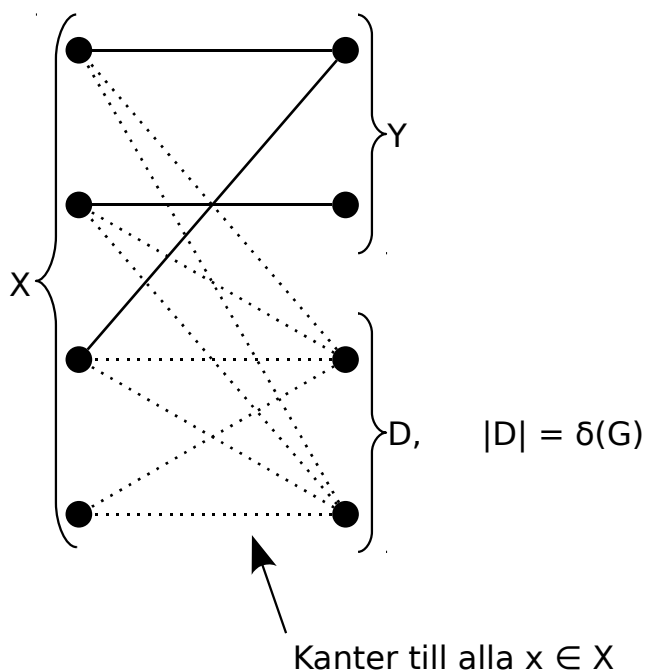
$$\delta(G) = \max_{A \subseteq X} \{|A| - |P(A)|\} \geq 0, \quad G\text{:s defekt (G:s underskott)}$$

Ty:

$$\delta(G) \geq 0, \text{ ty } A \neq \emptyset \text{ ger } |A| - |P(A)| = 0$$

$\delta(G) = 0$ omm villkoret i Halls sats är uppfyllt.

Om $\delta(G) > 0$: Utvidga G till $G^* = (X \cup (Y \cup D), E^*)$ enligt



Då är $A \neq \emptyset$

$$\begin{aligned} |P^*(A)| &= |P(A)| + |D| = \\ &= |P(A)| + \delta(G) \geq \\ &\geq |A| - \delta(G) + \delta(G) = |A| \end{aligned}$$

G^* har en fullständig matchning M^* (Halls sats) som ger en matchning med $|M| \geq |X| - \delta(G)$ i G och minst $\delta(G)$ är omatchad:

$$|A_0| = |P(A_0)| + \delta(G), \quad \text{något } A_0 \subseteq X$$

Sats:


En matchning M i en bipartit graf G är maximal om det inte finns en utökande alternerande stig för M i G . (Ger en algoritm för att finna maximal matchning.)

Ty:

\Rightarrow : Klart (en utökande alternerande stig utökar matchningen).

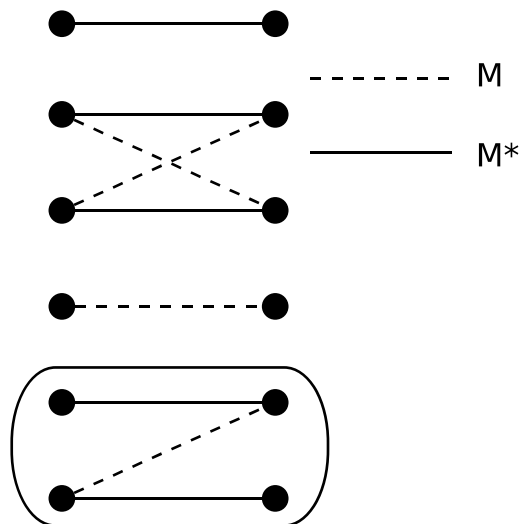
\Leftarrow : Om M inte är maximal, låt M^* vara det, $|M^*| > |M|$.
Vi skall visa att det finns en utökande alternerande stig.

Låt $F = M \Delta M^*$

 Symmetrisk differens, det vill säga kanter i exakt en av M och M^* .

Betrakta $G' = (X \sqcup Y, F)$, valenser 0, 1, 2 (inga andra) inte två kanter i M eller två kanter i M^* till ett hörn.

G' 's komponenter är alternerande stigar eller cykler, någon av dem har fler kanter från M^* . En utökande alternerande stig för M .



2011-(05)maj-17: dag 8, 30

Övning 10; graffärgning och matchningen.

Men först från förra KS:en:

Vi söker $2^{5^{2011}} \pmod{13}$

1) Använd Fermats lilla sats:

$$2^{12} \equiv 1 \pmod{13} \quad \text{Ty: } \begin{array}{l} 13 \text{ är ett primtal} \\ 12 \mid 13 - 1, 13 \nmid 2 \end{array}$$

$$5^{2011} \pmod{12}?$$

$$5^2 = 25 \equiv 1 \pmod{12}$$

Så:

$$5^{2011} = 5^{2 \cdot 1005 + 1} = (5^2)^{1005} \cdot 5 \equiv 1^{1005} \cdot 5 = 5 \pmod{12}$$

Så:

$$5^{2011} = k \cdot 12 + 5 \quad \text{och} \quad 2^{5^{2011}} = (2^{12})^k \cdot 2^5 \equiv 1^k \cdot \underbrace{2^5}_{32} \equiv 6 \pmod{13}$$

$$2) \quad 2^5 \equiv 6 \pmod{13}$$

$$6^5 = 36 \cdot 36 \cdot 6 \equiv (-3)^2 \cdot 6 = 54 \equiv 2 \pmod{13}$$

$$2^{5^{2011}} = \left((2^5)^5 \right)^5 \dots = \left(\underbrace{\left(\underbrace{(2^5)^5 \dots}_{2010} \right)^5}_{\equiv 2 \pmod{13}} \right)^5 \equiv 2^5 \dots \pmod{13}$$

Övningsuppgifter

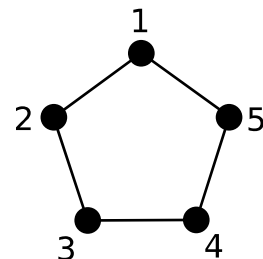
1) Kromatiska polynomet $P_{C_5}(\lambda)$ för C_5 ?

Med "kombinatoriskt resonemang":

$$\begin{aligned}
 P_{C_5}(\lambda) &= \lambda \cdot (\lambda - 1) \cdot [1 \cdot (\lambda - 1)(\lambda - 2) + (\lambda - 2)[1 \cdot (\lambda - 1) + (\lambda - 2)(\lambda - 2)]] = \\
 &= \lambda(\lambda - 1)(\lambda - 2)[\lambda - 1 + \lambda - 1 + (\lambda - 2)^2] = \\
 &= \lambda(\lambda - 1)(\lambda - 2)[(\lambda - 1)^2 + 1]
 \end{aligned}$$

Diagram illustrating the reasoning for the chromatic polynomial of C_5 :

- hörn 1: points to the first vertex (1)
- 5 som: points to the second vertex (2)
- 5 inte som 2, 1: points to the third vertex (3)
- 3 som: points to the fourth vertex (4)
- 3 inte som: points to the fifth vertex (5)



Alternativt med rekursionsformeln:

$$P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda)$$

$$\begin{aligned}
 P_{C_5}(\lambda) &= P_{T_5}(\lambda) - P_{C_4}(\lambda) = P_{T_5}(\lambda) - (P_{T_4}(\lambda) - P_{C_3}(\lambda)) = \\
 &= \lambda(\lambda - 1)^4 - \lambda(\lambda - 1)^3 + \lambda(\lambda - 1)(\lambda - 2) = \\
 &= \lambda(\lambda - 1)[(\lambda - 1)^3 - (\lambda - 1)^2 + (\lambda - 2)] = \dots
 \end{aligned}$$

Man kan verifiera att

$$P_{C_5}(\lambda) = (\lambda - 1)^5 + (-1)^5(\lambda - 1)$$

Vilket visades på föreläsning.

2)

Utgå från $P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda)$ och visa att $P_G(\lambda)$ är ett polynom med högstgradstermen λ^n , $n = |V|$, och nästgradstermen $-|E|\lambda^{n-1}$.

$G - e$ (G med kanten e borttagen) och G/e (G med kanten e ihopdragen (kontraherad)) har båda en kant mindre än G . Vi kan visa påståendet med induktion över $|E|$.

Bas:

Om G skanar kanter, $G = (V, \emptyset)$, $|V| = n$
 $P_G(\lambda) = \lambda^n$ OK!

Steg:

Antag att påståendet är sant för alla grafer med högst k stycken kanter.

Låt $G = (V, E)$ ha $|E| = k + 1$
 e är en kant i G ($e \in E$)

Induktionsantagande

$$P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda) \stackrel{IA}{=} \lambda^n - k\lambda^{n-1} + (...) - (\lambda^{n-1} + (...)) =$$

λ^{n-2} eller lägre

$$= \lambda^n - (k + 1)\lambda^{n-1} + (...)$$

Så påståendet är sant för $|E| = k + 1$.

- 4) Om transversaler (så Halls sats formulerades först) (boken DMF sida 244) att finna "distinkta representanter" med $m_i \in M_i$ och $m_i \neq m_j$ om $i \neq j$. Finns de?

Halls sats säger att det går omm

$$\left| \bigcup_{i \in A} M_i \right| \geq |A| \text{ för alla } A \subseteq I, I \text{ ändlig.}$$

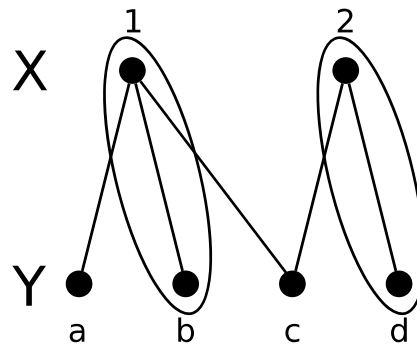
Ty:

Vi söker en fullständig matchning i en bipartit graf med

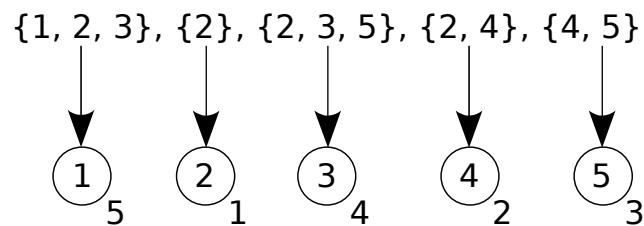
$$X = I, Y = \bigcup_{i \in I} M_i \quad \text{och}$$

kanter mellan $i \in I$ och alla element i M_i ,

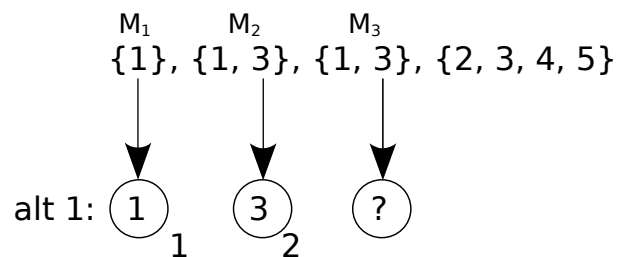
$$M_1 = \{a, b, c\}, \quad M_2 = \{c, d\}.$$



Vi söker en transversal till mängderna

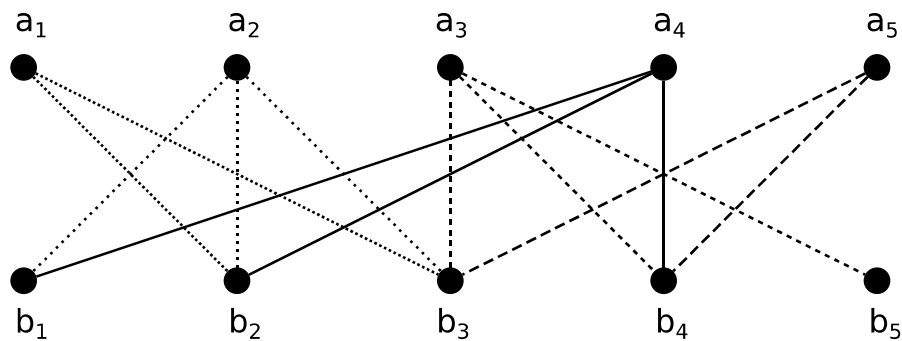


Varför finns ingen transversal till

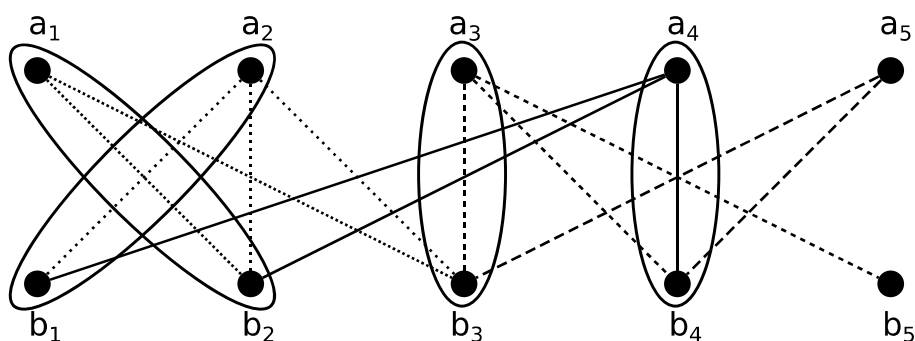


alt 2: Halls sats mängderna 1, 2, 3 har bara två element tillsammans, det vill säga färre element tillsammans än antalet mängder: ingen transversal.

5) Vi söker en fullständig matchningen till grafen

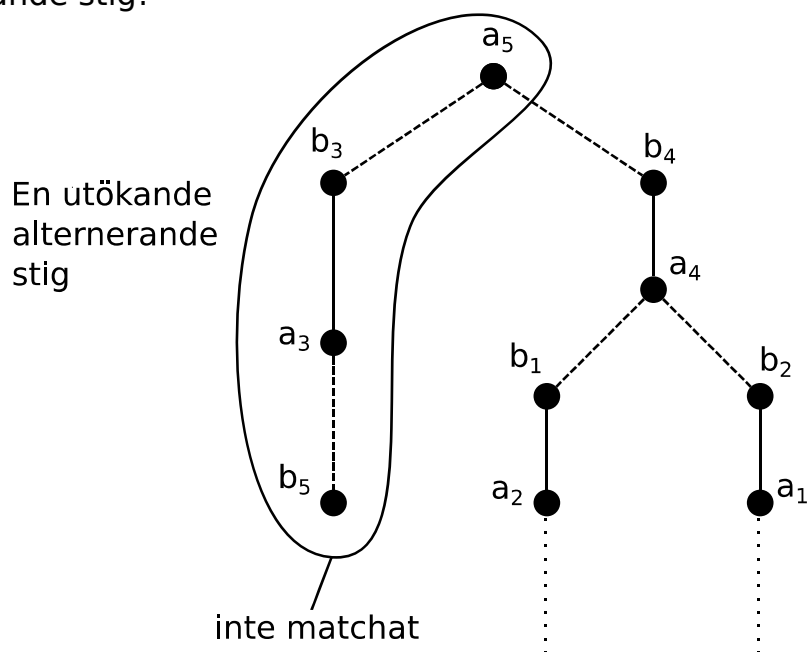


Efter 4 steg fås den ritade matchningen (nedan).
(Första lediga partiella matchningen tages, för varje a.)

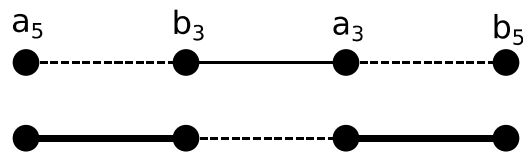


Hur skall a_5 matchas?

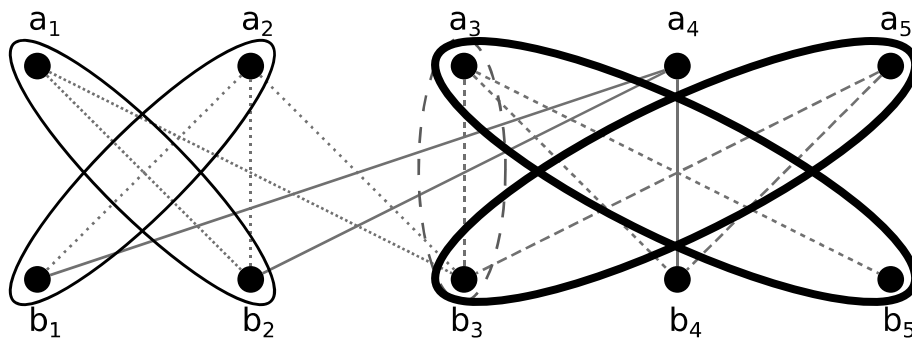
Sök en utökande alternerande stig!



Byt i den alternerande stigen.



Ger:



- 9) 10 skrivande, 10 uppgifter.
 Varje skrivande klarade minst 4 uppgifter.
 Varje uppgift klarades av minst 5 skrivande.

A en mängd skrivande, $A \neq \emptyset$, $|P(A)| \geq 4$ (alla klarade minst 4)

└─ Mängden uppgifter som någon i klarade.

$|A| > 4$ ger $|P(A)| = 10$

Varje uppgift klarades av ingen i A .
 Så $|P(A)| \geq |A|$ för alla A — Halls sats...

Supplement

Supplementära anteckningar, modul 1

Beviset för heltalsdivision med (principal) rest visar med små modifikationer att motsvarande gäller för polynom med rationella, reella eller komplexa koefficienter.

Resten $r(x)$:s grad $<$ delaren (divisorn) $d(x)$:s grad.

De Gaussiska heltalen $= \{m + in \mid m, n \text{ heltal}\}$ (i = den imaginära enheten).
 $|r()|^2 < |d()|^2$ för Gaussiska heltal $()$.

Talbas 8 kallas för det oktala talsystemet (talbas 10 kallas decimala talsystemet).

Delargrafter kallas också Hassediagram.

Supplementära anteckningar, modul 2

Betingade sannolikheten $P(A|B) = \frac{P(A \cap B)}{P(B)}$

$P(A|B) = P(A)$ omm A, B oberoende.

Supplementära anteckningar, modul 5

En graf kallas Eulersk, eller en Eulergraf, omm den har en Eulerkrets.

En graf kallas Hamiltonsk, eller, en Hamiltongraf, omm den har en Hamiltoncykel.

Sammanfattningar

Sammanfattning, modul 1: dag 1-7, 1-7

Division med rest:

Om p , d är heltal, $d \neq 0$ så finns entydiga heltal q , r så att
 $p = qd + r$, $0 \leq r < |d|$.

q kallas kvoten av p och d .
 r kallas (den principala) resten.

Ett (naturligt) tal kan skrivas i bas t ($t \geq 2$):

$$\begin{aligned}x &= q_0 t + r_0 \\q_0 &= q_1 t + r_1 \\&\vdots \\q_{n-2} &= q_{n-1} t + r_{n-1} \\q_{n-1} &= q_n t + r_n\end{aligned}$$

$$x = (r_n r_{n-1} \dots r_2 r_1 r_0)_t \quad r_i \text{ är siffror.}$$

$t = 2$ ger binär form	siffror:	01
$t = 8$ ger oktal form	siffror:	01234567
$t = 10$ ger decimal form	siffror:	0123456789
$t = 16$ ger hexadecimal form	siffror:	0123456789ABCDEF
	eller	0123456789abcdef

Andra, kanske bättre, siffror för A, B, C, D, E, F har funnits förr.

I andra baser än 10 ska siffrorna uttalas
separat (10 = ett noll, inte tio).

Om a , b är heltal betyder $a \mid b$ ("a delar b") att $b = qa$, q heltal.

Ett primtal är ett heltal $p > 1$ som bara har delarna ± 1 , $\pm p$.

Största gemensam delare (sgd, gcd på engelska):

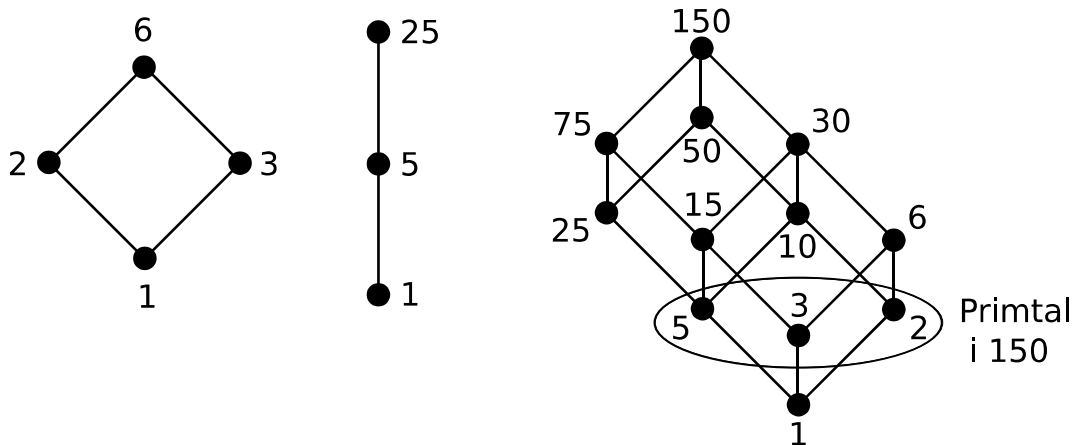
Största d så att $d|m$ och $d|n$.

Ger att $d = am + bn$ a, b heltal.

$$\text{sgd}(m; n) = \text{sgd}(n; m) = \text{sgd}(\pm n, \pm m)$$

Delargrafen för ett heltal $g > 0$:

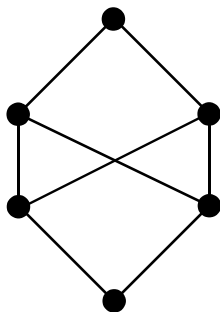
Punkter svarar mot all talets delare,
uppåtriktade streck från "direkta delare"



En gemensam delare till m, n i en delargraf:

Ett tal ligger under båda

Att det finns en entydig största gemensamma delare ger ett villkor på hur delargrafen kan se ut.



Finns ingen sådan delargraf.
Ty 0 saknar sgd.

Euklides' algoritm:

$$\text{sgd}(m; n) = \text{sgd}(n; m - qn) \quad \text{heltal } q$$

Detta medför:

$$\begin{array}{ll} m = q_1 n + r_1 & 0 \leq r_1 < n \\ n = q_2 r_1 + r_2 & 0 \leq r_2 < n \\ r_1 = q_3 r_2 + r_3 & 0 \leq r_3 < n \\ \vdots & \vdots \end{array}$$

$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$$

$$r_{k-2} = q_k r_{k-1} + 0$$

$$\text{sgd}(m; n) = r_{k-1}$$

Två heltal, m och n , är relativt prima om $\text{sgd}(m; n) = 1$. Alltså om $m \nmid n$ och $n \nmid m$.

Minsta gemensam multipel (mgm; lcm på engelska):

$\text{mgm}(a; b) = m$ så att $a \mid m$ och $b \mid m$, minsta m .

$$\text{mgm}(a; b) \cdot \text{sgd}(a; b) = ab$$

En diofantisk ekvation är en ekvation där endast heltalslösningar sökes.

Den linjära diofantiska ekvationen

$$ax + by = c \quad a, b, c \text{ heltal}$$

är lösbar omm (om och endast om; precis om; exakt om) $\text{sgd}(a; b) \mid c$.

Om lösbar, men inte $a = b = 0$, och $\text{sgd}(a; b) = d = ma + nb$, m, n heltal

$$\text{så ges alla lösningar av } \begin{cases} x = \frac{c}{d}m + \frac{b}{d}q \\ y = \frac{c}{d}n - \frac{a}{d}q \end{cases}, q \text{ hetal.}$$

Aritmetikens fundamentalsats:

Alla positiva heltal (större än 1) kan faktoriseras till en unik mängd av (icke-unika) primtal. (1 är "den tomma produkten".)

Om $a = p_1^{s_1} \dots p_k^{s_k}$, $b = p_1^{t_1} \dots p_k^{t_k}$ så är

$\text{sgd}(a; b) = p_1^{\min(s_1; t_1)} \dots p_k^{\min(s_k; t_k)}$ och $\text{mgm}(a; b) = p_1^{\max(s_1; t_1)} \dots p_k^{\max(s_k; t_k)}$

Modulär aritmetik:

$x \equiv y \pmod{m}$ eller $x \equiv_m y$ eller $x = y \text{ i } \mathbb{Z}_m$

(Sista bara för heltal, för andra mängder måste man byta ut \mathbb{Z} .)

betyder $m|(x - y)$, och läses "x är kongruent med y modulo m".

$$x_1 \equiv_m x_2, y_1 \equiv_m y_2 \Rightarrow x_1 + y_1 \equiv_m x_2 + y_2, x_1 y_1 \equiv_m x_2 y_2$$

$r \text{ i } \mathbb{Z}_m$ är inverterbart om $x \in \mathbb{Z}_m$ så att $rx = 1 \text{ i } \mathbb{Z}_m$.

$x = r^{-1}$ r:s invers.

r är inverterbart om $\text{sgd}(r; m) = 1 \text{ (i } \mathbb{Z}_m)$.

Om m är ett primtal så är alla tal utom 0 inverterbart.

En mängd kan ses som en "påse" med "saker" (eller pekare till saker), dessa "saker" kallas element.

Två mängder är lika om de innehåller samma element.
Elementen i en mängd är oordnade.

$\{1, 2\}$ är mängden med talen 1 och 2.

$\{x \mid Px\}$ är mängden av alla tal med egenskapen P, till exempel:

$\{x \mid x > 4\}$ är mängden med alla tal som är strikt större än 4.

Den tomma mängden är mängden utan element, och betecknas \emptyset
 $\emptyset = \{x \mid x \neq x\} = \{\}$.

$\{\emptyset\} \neq \emptyset$, \emptyset är tom, $\{\emptyset\}$ är mängden som innehåller den tomma mängden.

Universum, \mathcal{U} , är grundmängden med alla element vi sysslar med.

Standardbeteckningar för olika talmängder: $\mathbb{Z}, \mathbb{N}, \mathbb{Z}_+, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

$a \in A$	a är ett element i A.	
$a \notin A$	a är inte ett element i A.	
$B \subseteq A$	B är en delmängd av A.	Alla element i B finns i A.
$B \subset A$	B är en äkta delmängd av A.	$B \subseteq A$, men $B \neq A$.
$ A $	A:s kardinalitet.	Antalet element i A.
$A \cup B$	Unionen av A och B; mängden med alla element i A eller B.	
$A \cap B$	Snittet (skärningen) av A och B; mängden med de element som finns i både A eller B.	
$A \setminus B$	Differensen mellan A och B; mängden med alla element som finns i A förutsatt att elementet inte finns i B.	
A^c	Komplementet till A; mängden med alla element som inte finns i A, (men finns i grundmängden (universum)).	
$\mathcal{P}(A)$	A:s potensmängd; mängden av alla A:s delmängder.	
$A \times B$	Produktmängden av A och B; mängden med alla elementpar mellan A och B, det vill säga $\{(a; b) \mid a \in A, b \in B\}$.	

$$C \subseteq A, A \subseteq B \Rightarrow C \subseteq B$$

Associativa lagen: $(A \cup B) \cup C = A \cup (B \cup C)$
 $(A \cap B) \cap C = A \cap (B \cap C)$

Kommutativa lagen: $A \cup B = B \cup A$
 $A \cap B = B \cap A$

Distributiva lagen: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgans lag: $(A \cup B)^c = A^c \cap B^c$
 $(A \cap B)^c = A^c \cup B^c$

Identitetslagar: $A \cup A = A$
 $A \cap A = A$
 $A \cap \mathcal{U} = A$
 $A \cup \emptyset = A$

Absorptionslagen: $A \cup (A \cap B) = A$
 $A \cap (A \cup B) = A$

Dubbelt komplement: $(A^c)^c = A$

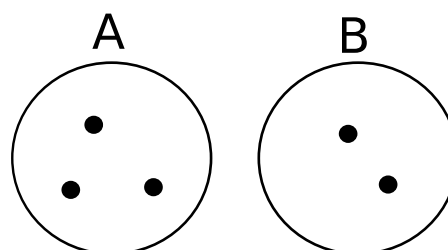
Inverslagar: $A \cup A^c = \mathcal{U}$
 $A \cap A^c = \emptyset$

Dominanslagar: $A \cap \emptyset = \emptyset$
 $A \cup \mathcal{U} = \mathcal{U}$

($A \cap B = B$ omm $B \subseteq A$)
($A \cup B = B$ omm $B \supseteq A$)

Om A, B disjunkta ($A \cap B = \emptyset$):

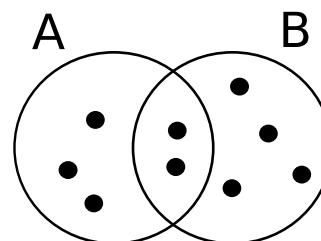
$$|A \cup B| = |A| + |B|$$



I allmänhet: (ej disjunkta eller disjunkta)

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

9
5
6
2



Induktionsbevis:

Om $P(a)$ är sant och om $P(n) \Rightarrow P(n + 1)$
så är $P(x)$ sant för alla heltal $x \geq a$.

Rekursion:

En följd har en eller fler fördefinierade värden,
startvärden. Till exempel: $F_0 = 0$, $F_1 = 1$

Nästa tal i möljden bestäms av föregående.
Till exempel:

$$F_n = F_{n-1} + F_{n-2}$$

(Detta är Fibonaccitalen.)

Funktioner, avbildningar

$$f : X \rightarrow Y, \quad y = f(x)$$

Sammansättning av funktion

$$f : X \rightarrow Y, \quad g : Y \rightarrow Z \quad \text{ger} \quad gf : X \rightarrow Z, \quad (gf)(x) = g(f(x))$$

gf brukar, mer tydligt, skrivas $g \circ f$

Den funktion $f : X \rightarrow Y$ kan definieras som en delmängd $f \subseteq X \times Y$ med

$$(x; y_1), (x; y_2) \in f \Rightarrow y_1 = y_2$$

För alla $x \in X$ finns $y \in Y$ så att $(x, y) \in f$

$f : X \rightarrow Y$ är en

injektion om har högst en $x \in X$ för alla $y \in Y$

surjektion om har minst en $x \in X$ för alla $y \in Y$

bijektion om har exakt en $x \in X$ för alla $y \in Y$ (injektion och surjektion).

Sammansättning av två -jektioner ger en -jektion (in-, sur-, bijektion)

$g : Y \rightarrow X$ är en inversfunktion, f^{-1} , till $f : X \rightarrow Y$ omm $(fg = f \circ g) \quad fg = \text{id}_Y, \quad gf = \text{id}_X$,
där $\text{id}_\Lambda(\lambda) = \lambda$ för alla $\lambda \in \Lambda$. (Λ är X eller Y)

f har en inversfunktion (är inverterbar) omm f är en bijektion,
 f^{-1} är också en bijektion.

Två mängder, X och Y , har samma kardinalitet
om det finns en bijektion $f : X \rightarrow Y$.

En mängds kardinalitet är entydig.

$|X| = n$ (kardinaliteten, antalet element = n)
betyder att det finns en bijektion
 $f : \{1, 2, \dots, n\} \rightarrow X$.

Att X är uppräknelig (uppräkneligt oändligt) betyder att det finns
en bijektion $f : \mathbb{N} \rightarrow X$.

\mathbb{Q} (de rationella talen) är uppräknelig

\mathbb{R} (de reella talen) är oändlig, men inte uppräknelig (den är överuppräknelig)

$|\mathbb{Q}| = |\mathbb{N}| < |\mathbb{R}|$

För alla mängder, ändliga som oändliga, X , gäller att:

$$|X| < |\mathcal{P}(X)|$$

Om \mathcal{R} är en binär relation på mängden X är $a\mathcal{R}b$ antingen sann eller falsk, för alla $a, b \in X$.

Relationen \mathcal{R} kan beskrivas med

en delmängd till X^2 , $\{(a; b) \in X^2 \mid a\mathcal{R}b\}$.

en graf med punkter svarande mot elementen i X och en pil från a till b omm $a\mathcal{R}b$.

en matris med rader och kolonner svaradne mot X :s element, 1 i position ab omm $a\mathcal{R}b$, annars 0.

Viktiga egenskaper för binära relationer:

\mathcal{R} reflexiv: $x \mathcal{R} x$, $\forall x \in X$

\mathcal{R} symmetrisk: $x \mathcal{R} y \Leftrightarrow y \mathcal{R} x$, $\forall x, y \in X$

\mathcal{R} antisymmetrisk: $x \mathcal{R} y \wedge y \mathcal{R} x \Rightarrow x = y$, $\forall x, y \in X$

\mathcal{R} transitiv: $x \mathcal{R} y, y \mathcal{R} z \Rightarrow x \mathcal{R} z$, $\forall x, y, z \in X$

En ekvivalensrelation på en mängd X är en relation \mathcal{R} som är reflexiv, symmetrisk och transitiv.

En ekvivalensrelation delar in X i ekvivalensklasser av element som står i relationen till varandra:

$$\mathcal{C}_x = [x] = \{y \in X \mid y\mathcal{R}x\}$$

En partialordning är en relation på mängden X som är reflexiv, antisymmetrisk och transitiv.

Om \leq är en partialordning på mängden X och $a \in X$ så är a

ett minimalt element i X om det inte finns $x \in X$ med $x \leq a$, $x \neq a$.

ett minsta element om $a \leq x$ för alla $x \in X$.

Motsvarande för maximala och största element.

Det finns antingen 0 eller 1 minsta element i X , samma sak gäller största element.

Sammanfattning, modul 2: dag 1-5, 8-12

Postfacksprincipen:

Om $|X| = n > |Y| = m$ så finns ingen injektion $f : X \rightarrow Y$.

“Om $n > m$ och n saker läggs i m låder, får minst en låda minst två saker.”

Additionsprincipen:

För ändliga, disjunkta A, B ($A \cap B \neq \emptyset$) gäller:

$$|A \cup B| = |A| + |B|$$

För flera ändliga, disjunkta A_i ($A_i \cap A_j \neq \emptyset, i \neq j$) gäller:

$$|A_1 \cup \dots \cup A_n| = |A_1| + \dots + |A_n|$$

Principen om inklusion/exklusion (sällprincipen):

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

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

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \dots + (-1)^{n+1} \alpha_n$$

$$\text{där } \alpha_i = \sum_{1 \leq k_1 < \dots < k_i \leq n} (A_{k_1} \cap \dots \cap A_{k_i})$$

Antalet med en viss egenskap = totala antalet – antalet utan egenskapen.

Om X, Y är mängder, $X \times Y = \{(x; y) \mid x \in X, y \in Y\}$

Sats: Om $S \subseteq X \times Y$, X, Y ändliga

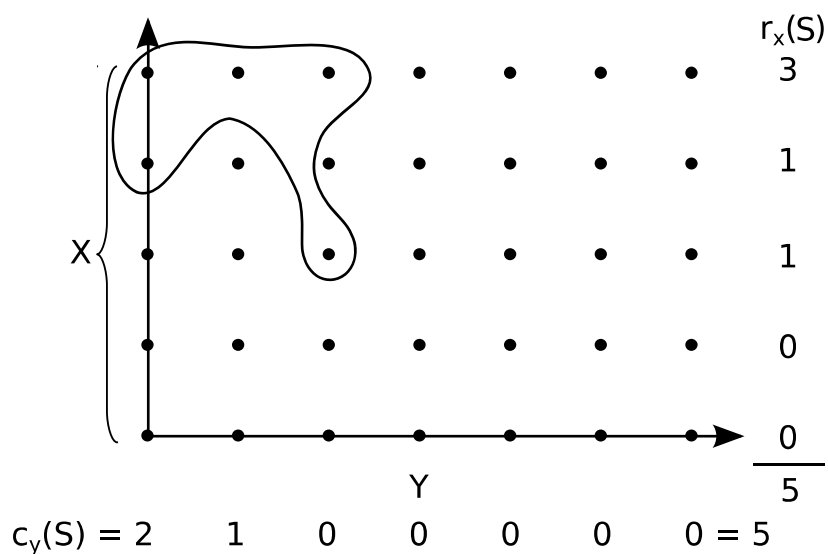
$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} c_y(S)$$

där $r_x(S) = |\{y \in Y \mid (x; y) \in S\}|$
 $c_y(S) = |\{x \in X \mid (x; y) \in S\}|$

radsumma
 kolumnsumma (kolonnsumma)

Multiplicationsprincipen:

$$|X \times Y| = |X| \cdot |Y|$$



Sannolikheter

ω utfall

Ω utfallsrum

A händelse

$\omega \in \Omega$

$A \subseteq \Omega$

Om alla $\omega \in \Omega$ har samma sannolikhet (likafördelning) är sannolikheten för $A \subseteq \Omega$:

$$P(A) = \frac{|A|}{|\Omega|}$$

För två händelse, A, B :

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Omm A och B är disjunkta ($A \cap B = \emptyset$):

$$P(A \cup B) = P(A) + P(B)$$

Omm A och B är oberoende gäller:

$$P(A \cap B) = P(A) \cdot P(B)$$

Sannolikheten för A betingat att B inträffar:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Omm A och B är oberoende:

$$P(A|B) = P(A)$$

Om $|X| = m$, $|Y| = n$, ändliga:

Antalet funktioner $f : X \rightarrow Y =$

$=$ antalet element i $Y^m = Y \times \dots \times Y$ (m stycken Y) $=$

$=$ antalet ord av längden m i $Y =$

$=$ antalet ordnade val med upprepning av m stycken ur $Y =$

$= n^m = |Y|^{|X|}$

Antalet injektioner $f : X \rightarrow Y =$

$=$ antalet ord av längden m i Y utan upprepning

$=$ antalet ordnade val utan upprepning av m stycken ur $Y =$

$= n(n-1)\dots(n-m+1) = (n)_m = {}_n P_m = \frac{n!}{(n-m)!}$

Antalet bijektioner $f : X \rightarrow Y =$

$= \begin{cases} n! = n(n-1)\dots 2 \cdot 1 & \text{om } |X| = |Y| \\ 0 & \text{annars} \end{cases}$

Antalet k -delmängder till en n -mängd $=$

$=$ antalet oordnade val av k stycken från en n -mängd utan upprepning $=$

$=$ binomialtalet $\binom{n}{k}$, (läses "n över k"; en. "n choose k")

Antalet ordnade val av k stycken från en n -mängd med upprepning =
 = antalet sätt att skriva $k = x_1 + x_2 + \dots + x_n$, $x_i \geq 0$ =

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

Binomialtal:

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

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

$$\binom{n}{0} = \binom{n}{n} \quad \binom{n}{k} = \binom{n}{n-k}$$

Binomialsatsen:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

Multinomialtal:

$$\binom{n}{k_1, k_2, \dots, k_m} = \frac{n!}{k_1! k_2! \dots k_m!} = \left(k_i \geq 0, \sum_{i=1}^m k_i = n \right)$$

= antalet sätt att fördela n olika element i m olika lådor,
 med k_i stycken i låda i =

= antalet sätt att ordna en multimängd som har k_i exemplar av element i =

= antalet funktioner $f: [n] \rightarrow [m]$ som antar värdet i precis k_i gånger,
 (där $[r] = \{1, 2, \dots, r-1\}$)

↑

$[\cdot]$ skrivs även $\llbracket \cdot \rrbracket$

Multinomialatsen:

$$(x_1 + \dots + x_m)^n = \sum_{\substack{\sum k_i = n \\ k_i \geq 0}} \binom{n}{k_1, \dots, k_m} x_1^{k_1} \dots x_m^{k_m}$$

Genererande funktioner :

En talföljd $\{a_n\}_{n \in \mathbb{N}}$ motsvarar funktionen $g(x) = \sum_{n=0}^{\infty} a_n x^n$,
som kan användas för att bestämma a_n .

Se sida 2f för 2011-(02)feb-23, dag 11, för ett exempel.

Stirlingtalen (av andra slaget) $S(n; k)$:

Antalet partitioner (uppdelningar) av en
 n -mängd i precis k icke-tomma delar.

$S(n; k)$ bestäms rekursivt av:

$$\begin{cases} S(n; k) = S(n-1; k-1) + k \cdot S(n-1; k), & 1 < k < n \\ S(n; 1) = S(n; n) = 1, & n = 1, 2, \dots \end{cases}$$

Om $|X| = n$ och $|Y| = k$ så är antalet surjektioner $f: X \rightarrow Y = k! \cdot S(n; k)$.

Antalet ekvivalensrelationer på X = antalet partitioner av $X = \sum_{k=1}^{|X|} S(|X|; k)$

En partition av ett naturligt tal n (inte som en partition av en mängd)

$$n = n_1 + \dots + n_k, \quad n_1 \geq \dots \geq n_k \geq 1$$

Kan ses som en partition av n stycken identiska (inte särskiljbara) objekt.
Ett exempel på samband mellan antalen partitioner av olika slag:

Antalet partitioner av n i högst m delar =
= antalet partitioner av n i delar som alla är $\leq m$.

Sammanfattning, modul 3: dag 1-7, 13-19

$(G; *)$ är en grupp om

$$G1) \quad \forall x, y \in G : x * y \in G$$

“slutenhet”

$$G2) \quad \forall x, y, z \in G : (x * y) * z = x * (y * z)$$

“associativitet”

$$G3) \quad \exists I \in G : \forall x \in G : I * x = x * I = x$$

“identitetsselement”

$$G4) \quad \forall x \in G : \exists x^{-1} \in G : x * x^{-1} = x^{-1} * x = I$$

“invers”

Om det i en grupp $(G; *)$ gäller att

$$a * b = b * a$$

för alla $a, b \in G$, kallas G abelsk eller kommutativ.

Grupptabeller är latinska kvadrater.

$*$	x
a	b

Precis en gång i varje rad.
Även en gång i varje kolumn.

$$ax = ay \Rightarrow x = y \Leftarrow xa = ya$$

En grupp, G , är cyklisk om det finns ett element $g \in G$ sådant att varje element i G är av formen g^n , något $n \in \mathbb{Z}$.

Ett sådant g kallas en generator, ett genererande element för G .

$$G = \langle g \rangle$$

Om $o(g) = m$:

$$G = \{1, g, g^2, g^3, \dots, g^{m-1}\} \quad \text{ser ut som } (\mathbb{Z}_m; +).$$

alla olika

Om $G = \langle g \rangle$ gäller $|G| = o(g)$

$o(g) = \infty$:

$$G = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\} \quad \text{ser ut som } (\mathbb{Z}; +).$$

Om $H \subseteq G$ och $(G; *)$ är en grupp så är H en delgrupp till G omm:

$$\begin{cases} S0: & H \neq \emptyset \\ S1: & x, y \in H \Rightarrow x * y \in H \\ S2: & x \in H \Rightarrow x^{-1} \in H \end{cases}$$

$Z(G) = \{z \in G \mid zg = gz, \text{ alla } g \in G\}$, G :s centrum

$C(g) = \{x \in G \mid xg = gx\}$ för alla $g \in G$

↖
"centralisatorn" till G

Sidoklasser (en. cosets)

Definition: Om H är en delgrupp till G , $g \in G$, så är $gH = \{gh \mid h \in H\}$ en vänstersidoklass till H (en. left coset) och $Hg = \{hg \mid h \in H\}$ en högersidoklass till H (en. right coset).

Sats:

Om H är en delgrupp till G så är g_1H och g_2H identiska eller disjunkta.

Ty: Låt $x \in g_1H \cap g_2H$, vi skall visa att $g_1H = g_2H$.

$x = g_1h_1 = g_2h_2$, $h_1, h_2 \in H$ så $g_1 = g_2h_2h_1^{-1}$ och om

$y \in g_1H \Rightarrow y = g_1(h \in H) = g_2h_2h_1^{-1}h (\in H) \Rightarrow y \in g_2H$

så
$$\left. \begin{array}{l} g_1H \subseteq g_2H \\ \text{på samma sätt } g_2H \subseteq g_1H \end{array} \right\} \Rightarrow g_1H = g_2H$$

De ger en partition av G (ekvivalensrelationen $g_2^{-1}g_1 \in H$)

(Om H är ändlig är) dessutom $|H| = |gH| = |Hg|$

Så Lagranges sats: Om G är ändlig, H en delgrupp till G :

$$|H| \mid |G|$$

$[G : H] = |G : H| = \frac{|G|}{|H|}$, H 's index i G , antalet (vänster eller höger) sidoklasser.

Om G är en grupp, $|G| = p$, p primtal så är G cyklisk.

En gruppisomorfi mellan $(G_1; *)$ och $(G_2; \circ)$ är en bijektion $\phi : G_1 \rightarrow G_2$ så att $\phi(g * g') = \phi(g) \circ \phi(g')$ för alla $g, g' \in G_1$.

Grupperna $(G_1; *)$, $(G_2; \circ)$ kallas isomorfa om det finns en isomorfi mellan dem.

$(G_1; *) \approx (G_2; \circ)$ (Beteckningen $(G_1; *) \cong (G_2; \circ)$ är mycket vanligare.)

Isomorfi är en ekvivalensrelation mellan grupper.

$$\begin{array}{l} \phi : \begin{array}{l} 0 \mapsto 1 \\ 1 \mapsto 2 \\ 2 \mapsto 0 \\ 3 \mapsto 5 \\ 4 \mapsto 3 \\ 5 \mapsto 4 \\ 6 \mapsto 6 \end{array} \end{array}$$

Enradsnotation: $\phi = [1 \ 2 \ 0 \ 5 \ 3 \ 4 \ 6]$

Tvåradsnotation: $\phi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 0 & 5 & 3 & 4 & 6 \end{pmatrix}$

Cykelnotation: $\phi = (0 \ 1 \ 2)(3 \ 5 \ 4)(6) = (0 \ 1 \ 2)(3 \ 5 \ 4)$

Ordningen för $\pi \in S_n$ är lätt att se av π :s cykelstruktur.

Exempel: $S_{12} \ni \pi = (1 \ 7 \ 4 \ 11)(2 \ 9 \ 6)(3 \ 5 \ 8 \ 12 \ 10)$

$o(\pi) = ?$

$4, 3, 5 \mid o(\pi)$ I varje cykel skall man gå ett helt antal varv.

”så” $o(\pi) = \text{mgm}(4, 3, 5) = 60$

Ett sätt till att beskriva permutationer:

$$\pi \in S_n \text{ motsvarar } \mathbf{M}_\pi \text{ med } m_{ij} = \begin{cases} 1 & \text{om } \pi(j) = i \\ 0 & \text{annars} \end{cases}.$$

$$\mathbf{M}_\pi = \begin{pmatrix} 0 & 0 \\ 0 & \vdots \\ \vdots & 0 \\ 0 & \dots & 1 \\ 1 & 0 \\ 0 & \vdots \\ \vdots & \\ 0 & \end{pmatrix}$$

kolonn j

rad $\pi(j)$

rad $\pi(i)$

så $\mathbf{M}_\pi \mathbf{e}_j = \mathbf{e}_{\pi(j)}$ där $\mathbf{e}_k =$

$$= \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

rad k

Och $\mathbf{M}_\pi \mathbf{M}_\sigma \mathbf{e}_j = \mathbf{M}_\pi \mathbf{e}_{\sigma(j)} = \mathbf{e}_{\pi(\sigma(j))} = \mathbf{e}_{(\pi\sigma)(j)} = \mathbf{M}_{\pi\sigma} \mathbf{e}_j$ så $\mathbf{M}_\pi \mathbf{M}_\sigma = \mathbf{M}_{\pi\sigma}$

\nwarrow \nwarrow \nwarrow
 $n \times n$ $n \times 1$

Multiplikation i S_n motsvarar matrismultiplikation.

$$\mathbf{M}_\pi^t = \mathbf{M}_\pi^{-1} \text{ (ortogonal matris) } = \mathbf{M}_{\pi^{-1}}$$

Cayleys sats:

Varje grupp G är isomorf med en delgrupp till S_G .

Ty: $\varphi : G \rightarrow S_G$ så att för $g, h \in G : \varphi(g)(h) = gh$ då

$$(\varphi(g_1) \circ \varphi(g_2))(h) = \varphi(g_1)(\varphi(g_2)(h)) =$$


$$= \varphi(g_1)(g_2h) = g_1(g_2h) =$$

$$= (g_1g_2)(h) = \varphi(g_1g_2)h \quad \text{så}$$

$$\varphi(g_1) \circ \varphi(g_2) = \varphi(g_1g_2)$$

$$\varphi \text{ injektiv ty } g_1h = g_2h \Rightarrow g_1 = g_2$$

$$\text{så } G \cong \varphi(G) = \{\varphi(g) \mid g \in G\}$$

 Isomorfi, skrivs ibland $G \approx \varphi(G)$.

(Speciellt kan varje ändlig grupp representeras med matriser.)

Konjugering i S_n

$\alpha, \beta \in S_n$ är konjugerade om det finns $\sigma \in S_n$ så att $\sigma\alpha\sigma^{-1} = \beta$
(det vill säga $\sigma\alpha = \beta\sigma$).

En ekvivalensrelation på S_n (reflexiv, symmetrisk och transitiv).

Exempel:

$$\sigma = (1\ 2\ 3)(4\ 5) \text{ är konjugerad till } \beta = (1\ 3)(2\ 4\ 5).$$

$$\sigma = (1\ 5\ 3\ 4) \text{ ger } \sigma\alpha\sigma^{-1} = (1\ 5\ 3\ 4)(1\ 2\ 3)(4\ 5)(1\ 4\ 3\ 5) = (1\ 3)(2\ 4\ 5)$$

$\alpha, \beta \in S_n$ är konjugerade om de har samma cykelstruktur.

Klasser av konjugerade element i S_n svarar precis mot partitioner av heltalet n .

Exempel: Alla element i S_5 konjugerade med $(1\ 4)(2\ 5\ 3)$ är de med cykelstruktur $[2\ 3]$.

Exempel: $\underbrace{\sigma\pi}_\beta = \sigma(\underbrace{\pi\sigma}_\alpha)\sigma^{-1}$, så $\sigma\pi$ och $\pi\sigma$ är konjugerade.

En grövre uppdelning av S_n : jämna och udda.

En transposition: en permutation av typ $[1^{n-2}\ 2]$, det vill säga (ij) $i \neq j$.

Om $\pi \in S_n$ så finns transpositioner τ_1, \dots, τ_r så att $\pi = \tau_r \tau_{r-1} \dots \tau_2 \tau_1$
ty $(x_1\ x_2 \dots x_k) = (x_1\ x_k)(x_1\ x_{k-1}) \dots (x_1\ x_2)$.

π är en jämn/udda permutation om r är jämnt/udda då $\pi = \tau_r \tau_{r-1} \dots \tau_1$;
 $\text{sgn } \pi = (-1)^r$.

Om $\pi \in S_n$, $\pi = \tau_r \tau_{r-1} \dots \tau_1 = \tau'_r \dots \tau'_1$ (τ_i, τ'_i transpositioner)
så har r och r' samma paritet. (Båda jämna eller båda udda.)

$(U(G), \cdot)$ är en grupp av $U(G)$, de invertibla elementen i G .

$$U(\mathbb{Z}_m) = \{r \in \mathbb{Z}_m \mid \text{sgd}(r, m) = 1\}$$

$(R, +, \cdot)$ är en ring om $(R, +)$ är en kommutativ grupp med identitetselement 0,
 (R, \cdot) är sluten och associativ med identitetselement 1 och \cdot distributiv över $+$.

$(F, +, \cdot)$ är en kropp (en. field) om $(F, +, \cdot)$ är en ring och
 $(F \setminus \{0\}, \cdot)$ är en kommutativ grupp.

$\phi : A \rightarrow B$ är en homomorfi mellan (A, \circ) och (B, \bullet) om

$$\phi(a \circ b) = \phi(a) \bullet \phi(b) \in B \quad \forall a, b \in A$$

En isomorfi är en bijektiv homomorfi.

Direkta produkten av (A, \circ) och (B, \bullet) :

$$(A, \circ) \times (B, \bullet) = (A \times B, *)$$

och

$$(a_1, a_2) * (b_1, b_2) = (a_1 \circ a_2, b_1 \bullet b_2)$$

N kallas en normal delgrupp till G om vänstersidoklasserna = högersidoklasserna.
Det vill säga om $gN = Ng \quad \forall g \in G$ (ekvivalent: $gNg^{-1} = N$).

Alla delgrupper till en abelskgrupp är normala delgrupper.

Då är $G/N = \{gN \mid g \in G\}$ en grupp, kvotgruppen.

$$g_1Ng_2N = \{h_1h_2 \mid h_1 \in g_1N, h_2 \in g_2N\} = g_1g_2N$$

S_n ($n \geq 2$) har hälften jämna och hälften udda permutationer.
De jämna permutationerna utgör en normal delgrupp till S_n ,
denna delgrupp kallas A_n .

För en $n \times n$ -matris \mathbf{A} :

$$\det \mathbf{A} = \sum_{\pi \in S_n} \text{sgn } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)} = \sum_{\pi \in S_n} \text{sgn } \pi a_{\pi(1)1} a_{\pi(2)2} \dots a_{\pi(n)n}$$

$$\det \mathbf{M}_\pi = \text{sgn } \pi$$

Sammanfattning, modul 4: dag 1-7, 19-25

Koden \mathcal{C} är en mängd n -tuper av 1:or och 0:or, alltså $\mathcal{C} \subseteq \mathbb{Z}_2^n$, n är kodens längd.

Minimala avståndet, δ , för \mathcal{C} :

$$\delta = \min\{d(a, b) \mid a, b \in \mathcal{C}, a \neq b\}, \quad d(a, b) = \text{antalet } i \text{ med } a_i \neq b_i$$

\mathcal{C} är felrättande och kan upptäcka upp till $\delta - 1$ fel,
men rätta upp till $\left\lfloor \frac{\delta - 1}{2} \right\rfloor$ fel (alltså avrundat nedåt).

Sfärpackningssatsen:

Om koden \mathcal{C} har längden n och rättar upp till e fel:

$$|\mathcal{C}| \left(\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{e} \right) \leq 2^n \quad (= |\mathbb{Z}_2^n|)$$

$|\mathcal{C}| = 2^k$, k är \mathcal{C} :s dimension.

\mathcal{C} är en linjär kod om $a, b \in \mathcal{C} \Rightarrow a + b \in \mathcal{C}$.

Det vill säga \mathcal{C} är ett delrum till \mathbb{Z}_2^n , en delgrupp till $(\mathbb{Z}_2^n, +)$.

Då är minimala avståndet = minimala (nollskilda) vikten, det vill säga

$$\delta = w_{\min} = \min\{w(c) \mid c \in \mathcal{C}, c \neq 0\}$$

$w(c)$, vikten för c , är antalet 1:or i c .

Om H är en $m \times n$ -matris är $\mathcal{C} = \{x \in \mathbb{Z}_2^n \mid Hx = 0\}$ är en linjär kod av dimension $n - \text{rank } H$. H allas kodens (paritets)kontrollmatris.

Om H 's alla kolonner är $\neq \vec{0}$ så rättar \mathcal{C} minst ett fel.

z är ett kodord med fel i position $i \Rightarrow Hz = H$'s i :e kolonn.

Hammingkoder ges av en kontrollmatris H med r rader och $2^r - 1$ kolonner, alla olika och $\neq \vec{0}$ (alla som finns).

Längd:	$n = 2^r - 1$
Minimiavstånd:	$\delta = 3$
Dimension:	$k = 2^r - r - 1$

Hammingkoder ger likhet i sfärpackningstatsen, de är perfekta koder.

Är (det stora) talet N ett primtal?

Fermattest (bas b , $1 < b < N$):

Är $b^{N-1} \equiv 1 \pmod{N}$?

Nej: N är sammansatt. Ja: Vet inte.

Pseudoprimtal, bas b :

Sammansatt, klarar Fermattestet, bas b .

Exempel: $341 = 11 \cdot 31$, bas 2

Carmichaeltal:

Klarar alla Fermattest med bas b med $\text{sgd}(b, N) = 1$.

N är ett Carmichaeltal omm det är kvadratfritt och
 $p \mid N \Rightarrow p^{-1} \mid N - 1$.

Starkare test:

Miller-Rabins test (M-R)

Förfinning av Fermattestet:

$$N - 1 = n \cdot 2^r, \quad n \text{ udda}, r \geq 1 \text{ (} N \text{ udda)}$$

M-R:

$$b^n \pmod{N}$$

$$(b^n)^2 \pmod{N}$$

$$\left((b^n)^2\right)^2 = b^{n \cdot 2^2} \pmod{N}$$

\vdots

$$b^{n \cdot 2^r} \equiv 1 \pmod{N}$$

Om N klarar Fermattestet, bas b .

Om N är ett primtal

$$b^n \equiv 1 \pmod{N}$$

eller

$$(b^n)^{2^i} \equiv -1 \pmod{N}, \quad \text{något } i, 0 \leq i < r.$$

Satslogik

En sentens är en symbolsträng som kan stå för olika utsagor (påståenden).
Sentener byggs upp av atomära sentenser, konnektiv och parenteser.

1 = T, t, s = Sant
0 = F, f, f = Falskt

Sanningsvärdestabeller:

p	$\neg p$
1	0
0	1

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

$p \wedge q$:	1 omm båda 1	»båda sanna»
$p \vee q$:	0 omm båda 0	»någon sann»
$p \rightarrow q$:	0 omm (1, 0)	»q minst lika sann som p»
$p \leftrightarrow q$:	1 omm lika	»p och q lika sanna»

Kontraposition: $p \rightarrow q \equiv \neg p \rightarrow \neg q$
Omvändning: $p \rightarrow q \not\equiv q \rightarrow p$

Sanningsvärdestabeller för “större” sentenser

A B C	$C \rightarrow (A \wedge \neg B)$ $C \rightarrow A \wedge \neg B$			$(C \rightarrow A) \wedge \neg(B \wedge C)$		
1 1 1	0	0	0	1	0	1
1 1 0	1	0	0	1	1	0
1 0 1	1	1	1	1	1	0
1 0 0	1	1	1	1	1	0
0 1 1	0	0	0	0	0	1
0 1 0	1	0	0	1	1	0
0 0 1	0	0	1	0	1	0
0 0 0	1	0	1	1	1	0

hela

$A \wedge \neg B$

$\neg B$

hela

$C \rightarrow A$

$\neg(B \wedge C)$

$B \wedge C$

(1)
(2)
(3)

Observera att i exemplet får båda satsenerna samma sanningsvärden i alla tolkningar (alla rader). Vi säger att satsenerna är logiskt ekvivalenta.

$$C \rightarrow A \wedge \neg B \equiv (C \rightarrow A) \wedge \neg(B \wedge C)$$

(\Leftrightarrow i boken; = för +, ·, -notationen)

Boolesk algebra, enkla logiska ekvivalenser

$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$	kommutativitet
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	associativitet
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	distributivitet
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan
$p \wedge p \equiv p$	$p \vee p \equiv p$	idempotens
$p \wedge (p \vee q) \equiv p$	$p \vee (p \wedge q) \equiv p$	absorption

$\neg \neg p \equiv p$	involution
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$	\leftrightarrow uttryckt
$p \rightarrow q \equiv \neg p \vee q$	\rightarrow uttryckt
$\neg p \equiv p \rightarrow \perp$	\neg uttryckt

$p \wedge \neg p \equiv \perp$	komplementaritet
$p \wedge \perp \equiv \perp$	Alltid falsk (falsum)
$p \wedge \top \equiv p$	
	Alltid sann (verum)

Annat skrivsätt (x·y skrivs oftast xy)

$p \cdot q = q \cdot p$	$p + q = q + p$	kommutativitet
$(p \cdot q) \cdot r = p \cdot (q \cdot r)$	$(p + q) + r = p + (q + r)$	associativitet
$p \cdot (q + r) = (p \cdot q) + (p \cdot r)$	$p + (q \cdot r) = (p + q) \cdot (p + r)$	distributivitet
$\overline{p \cdot q} = \overline{p} \cdot \overline{q}$	$\overline{p + q} = \overline{p} \cdot \overline{q}$	De Morgan
$p \cdot p = p$	$p + p = p$	idempotens
$p \cdot (p + q) = p$	$p + (p \cdot q) = p$	absorption

$$\overline{\overline{p}} = p \quad \text{involution}$$

$$\begin{aligned} p \cdot \overline{p} &= \mathbf{0} & \text{komplementaritet} \\ p \cdot \mathbf{0} &= \mathbf{0} \\ p \cdot \mathbf{1} &= p \end{aligned}$$

Notera att $\overline{\overline{x} \cdot \overline{y}} \neq \overline{x} \cdot \overline{y}$ och $\overline{x} \cdot \overline{y} \neq \overline{x \cdot y}$

+ är inte likadan som i \mathbb{Z}_2 .

0-ställiga (en. nullary) konnektiv: \perp \top

1-ställiga (en. unary) konnektiv: \neg

2-ställiga (en. binary) konnektiv: \wedge \vee \rightarrow \leftrightarrow

$$\mathbb{B}_n = \{0, 1\}^n = \{00\dots 0, 00\dots 1, \dots, \underbrace{11\dots 1}_{\times n}\}$$

En boolesk funktion beskrivs fullständigt av en sanningsvärdestabell.

Exempel:

x	y	z	f(x, y, z)	
1	1	1	1	xyz 1 på denna rad, 0 för övriga
1	1	0	1	xy \bar{z} 1 på denna rad, 0 för övriga
1	0	1	1	x \bar{y} z 1 på denna rad, 0 för övriga
1	0	0	0	
0	1	1	0	
0	1	0	0	
0	0	1	1	$\bar{x}\bar{y}$ z 1 på denna rad, 0 för övriga
0	0	0	0	

“Så” $f(x, y, z) = xyz + xy\bar{z} + x\bar{y}z + \bar{x}\bar{y}z$

På samma sätt kan varje boolesk funktion skrivas på disjunktiv normalform (dnf).

Dualt: konjunktiv normalform (knf)

$$f(x, y, z) = (\bar{x} + y + z)(x + \bar{y} + \bar{z})(x + \bar{y} + z)(x + y + z)$$

Karnaugh-diagram

		Z	
		z	\bar{z}
xy	\bar{x}	0 0	0 1
	y	0 1	0 0
	x	1 1	1 1
	\bar{y}	1 0	0 1

Här är $f(x, y, z) = \underline{\bar{x}y} + \underline{\bar{y}z}$

För ihop 1:orna i rektanglar med sida 1, 2 eller 4 (2^n). Rektanglarna ska vara Så stora som möjlig som får vara överlappande.

Endast en skillnad per rad i xy, gäller även i kolonnerna.

I diagrammet till vänster finns, det två ihopförningar, de heldragna bilder en rektangel.

Dualitet: Om varken p eller q innehåller \rightarrow eller \leftrightarrow och $p = q$, så också $d(p) \equiv d(q)$, där $d(p)$ fås av att i p byta alla $\wedge \rightleftharpoons \vee$ och $\top \rightleftharpoons \perp$.

Kryptering

\mathcal{M} — Meddelande i klartext
 \mathcal{C} — Chiffer (Meddelandet krypterat)

$$E(\mathcal{M}) = \mathcal{C}, \quad D(\mathcal{C}) = \mathcal{M}, \quad D = E^{-1}$$

E — Krypteringsalgoritim (nyckel inbyggd)
D — Dekrypteringsalgoritim (nyckel inbyggd)

Traditionellt: E och D bara kända av behöriga, E och D kan fås ur varandra.
(symmetriskt krypto)

Modernt (1976): Offentlig nyckel, E kan inte (lätt) fås ur D och är offentlig.

(till exempel RSA, asymmetriskt krypto)

Asymmetriska krypton är söliga, och kan användas för att komma överrens om ett symmetriskt krypto.

Elektronisk signatur:

1. Offentliggör $D(x)$. Alla kan läsa (med E), ingen utan D kunde ha skrivit.
2. B änder $E_A(D_B(x))$ (eller $D_B(E_A(x))$) till A . Bara någon med D_A kan läsa, bara någon med D_B kunde ha skrivit.

Fermats lilla sats:

Om p är ett primtal och $p \nmid a$ så $a^{p-1} \equiv 1 \pmod{p}$.

Sats:

Låt p och q vara olika primtal, $n = pq$, $m = (p-1)(q-1)$.
 $s \equiv 1 \pmod{m} \Rightarrow x^s \equiv x \pmod{n}$, alla $x \in \mathbb{Z}$.

RSA-algoritmen:

Tag två stora primtal ($\approx 10^{150}$), p och q .

Välj e med $\text{sgd}(e, m) = 1$.

Finn d så att $ed \equiv 1 \pmod{m}$. (Euklides)

Offentliggör n och e och hemlighåll d .

$$E, D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

$$E(x) = x^e, \quad D(x) = x^d$$

$$D = E^{-1}$$

$E(x)$ och $D(x)$ kan beräknas med upprepad kvadrering \pmod{n} av x och multiplication \pmod{n} av rätt $x^{2^i} \pmod{n}$.

Sammanfattning, modul 5: dag 1-8, 23-30

En graf

“Teoretisk”, abstrakt

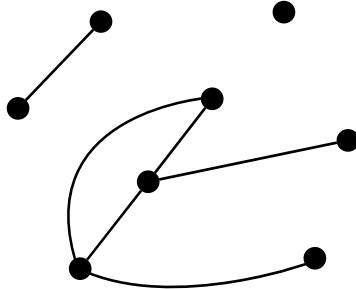
$$G = (V, E)$$

V — En ändlig mängd, hörn (noder, vertex)
(en. node, vertex (pluralis: vertices)).

E — En mängd av 2-delmängder till V , kanter
(en. edge), (par av olika hörn).

De hörnen är då grannar.

“Praktiskt”

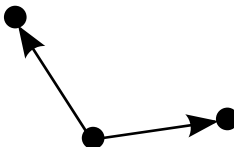


Enkla, oriktade grafer

Inga:

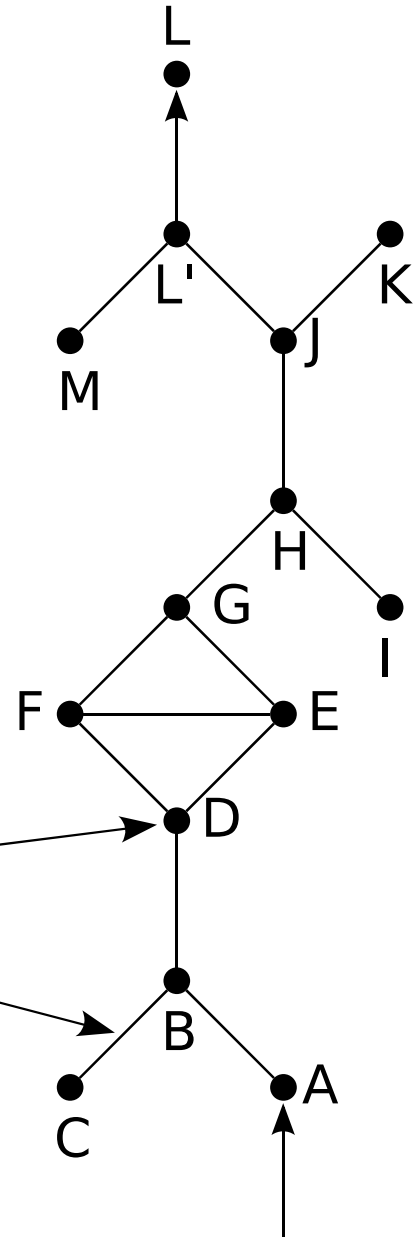


Inte:



hörn, $V \in D$

kant, $E \ni CB$



Varianter av grafer:

Oändlig mängder (hörn)

Riktade kanter

Viktade kanter

Öglor

Multipla kanter

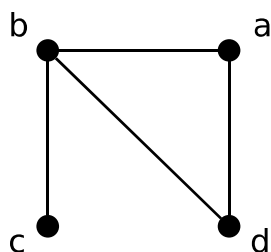
Standardnamn för vissa grafer:

K_n , fullständiga grafen med n hörn, $n \geq 1$
Alla möjliga kanter finns.

C_n , cykliska grafen med n hörn, $n \geq 3$

$K_{m,n}$, fullständiga bipartita grafen, $m, n \geq 1$
 $G = (A \sqcup B, E = \{ab : a \in A, b \in B\})$

Grannlista för en graf:



a	b	c	d
b	a	b	a
d	c		b
	d		

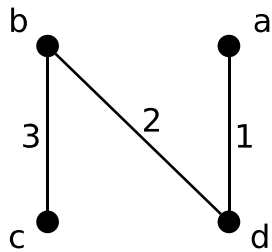
Grannmatris för samma graf:

	a	b	c	d
a	0	1	0	1
b	1	0	1	1
c	0	1	0	0
d	1	1	0	0

För enkel oriktad:
Symmetrisk 0/1-matris,
0:or på diagonalen.

$$a_{ij} = \begin{cases} 1 & \text{om } \{ij\} \in E \\ 0 & \text{annars} \end{cases}$$

Incidentmatris:



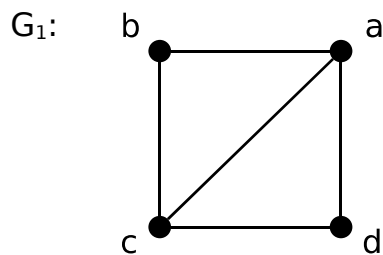
$$\begin{matrix} & 1 & 2 & 3 \\ \begin{matrix} a \\ b \\ c \\ d \end{matrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \end{matrix}$$

Isomorfi mellan grafer ("strukturlikhet")

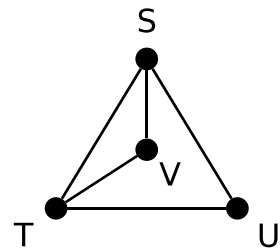
$G_1 = (V_1, E_1)$ är isomorfisk med $G_2 = (V_2, E_2)$ betyder att det finns en bijektion $\phi : V_1 \rightarrow V_2$ så att

$$\{x, y\} \in E_1 \Leftrightarrow \{\phi(x), \phi(y)\} \in E_2$$

Exempel:



och G_2 :



är isomorfa med isomorfi $\phi = \begin{pmatrix} a & b & c & d \\ S & V & T & U \end{pmatrix}$.

Valensen (graden) för ett hörn $v \in V$:

$\delta(v)$ = antalet kanter där v ingår, (öglor räknas dubbelt).

En graf är n -reguljär om alla hörn har valens n .

K_n är $(n - 1)$ -reguljär

C_n är 2-reguljär

Sats:

$$\sum_{v \in V} \delta(v) = 2|E|$$

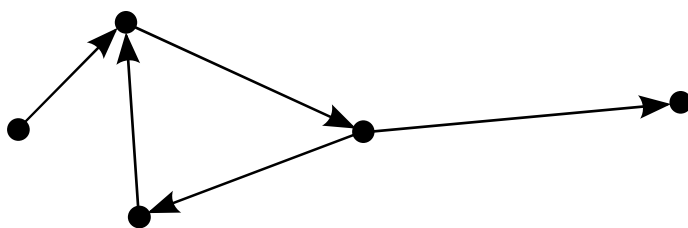
Följdsats:

Antalet udda hörn (det vill säga hörn med udda valens) är jämnt.

Namn för olika kantföljder i en graf:

Vandring (en. walk)

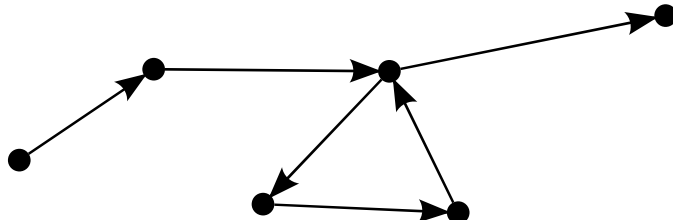
Från hörn till grannhörn. $\{v_i, v_{i+1}\} \in E, v_i \in V$.



Väg

(en. trail)

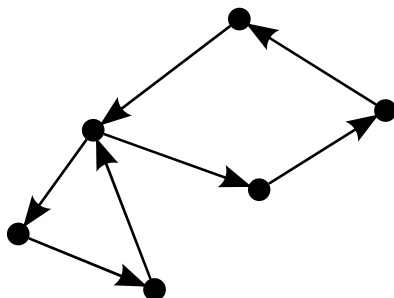
Vandring utan upprepade kanter.



Krets

(en. circuit)

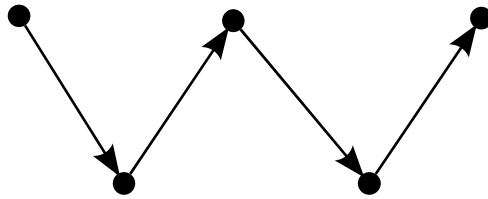
Sluten väg, $v_1 = v_k$



Stig

(en. path)

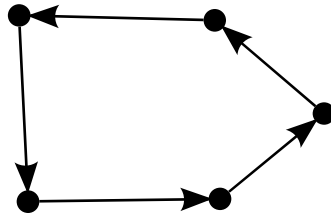
Väg utan upprepade hörn



Cykel

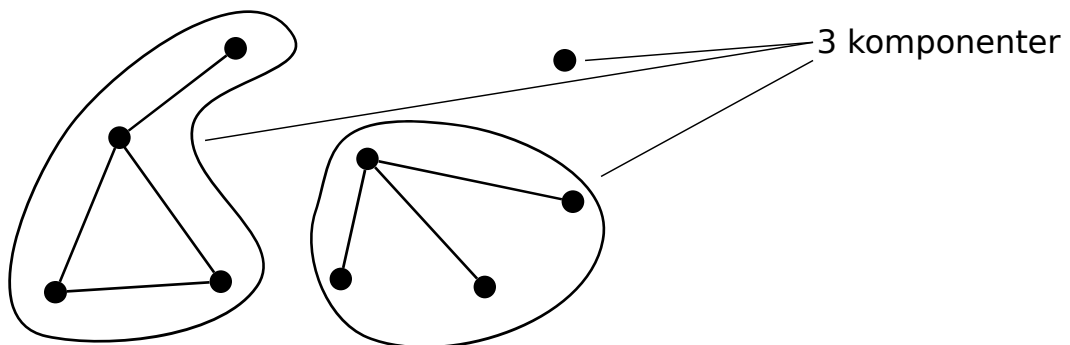
(en. cycle)

Sluten stig



En graf är sammanhängande om varje par hörn kan förbindas med en vandring, väg eller stig.

Relationen mellan hörn och att kunna förbindas är en ekvivalensrelation.
Ekvivalens klasser: grafens komponenter



En Eulerväg är en väg som passerar varje kant exakt en gång.

Sats: En graf, G , har en Eulerväg om G är sammanhängande och
(Euler) har högst 2 udda hörn.

G har en Eulerkrets om dessutom alla hörn är jämna.

Man kan sätta ihop en Eulerväg/-krets med flera Eulerkretsar.

En Hamiltonstig/-cykel passerar varje hörn i grafen precis en gång.

Varje komponent i en skog kallas träd:

Ett träd är sammanhängande och icke-cykliskt.

Träd brukar betecknas $T = (V, E)$

För en viktad sammanhängande graf (kant e har vikten $\omega(e)$) kan man finna ett minimalt spännande träd, ett spännande träd med minimal viktsumma, med Kruskals algoritm.

Kruskals algoritm:

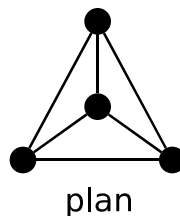
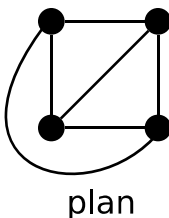
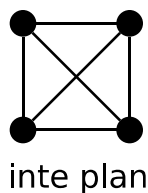
Lägg i varje steg till den lättaste kanten som inte ger någon cykel med de redan valda.

Planära grafer

Om en graf är ritad i ett plan *eller på en sfär* utan att några kanter korsar, så kallas grafen plan

En planär graf är en graf som är isomorf med någon plan graf.

Exempel på isomorfa planära grafer (K_4):



Sats:

För en plan graf med v hörn, e kanter, r ytor och c komponenter gäller:

$$v - e + r - c = 1 \quad (\text{mnemonik: verk!, naturligtvis med !})$$

Om grafen är sammanhängande ($c = 1$):

Eulers polyederformel:

$$v - e + r = 2$$

Satsen ger nödvändiga villkor för planaritet:

Om G , sammanhängande, är enkel (inga ölgör eller multipla kanter), så begränsas varje uta av minst tre kanter (om $e \geq 2$!).

$$\text{Så: } 2e = \sum_{\text{områden}} \underbrace{(\text{antalet kanter kring området})}_{\geq 3} \geq 3r$$

$$\text{Så: } e \geq \frac{3}{2}r \quad r \leq \frac{2}{3}e \quad \Rightarrow \quad e = v - e + r \leq v - \frac{1}{3}e$$

$$3v \geq e + 6$$

Kuratowskis sats:

Varje icke-planär graf "innehåller" K_5 eller $K_{3,3}$, och vice versa.

↓
det finns en delgraf som är isomorf med en "subdivision" av K_5 eller $K_{3,3}$.

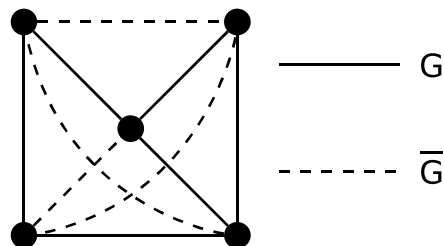
↓
Den graf med extra hörn på kanter.

Wagners sats:

Detsamma med "innehåller" betyder att den har K_5 eller $K_{3,3}$ som minor.
Det vill säga någon kantkontraktion av grafen har K_5 eller $K_{3,3}$ som delgraf.

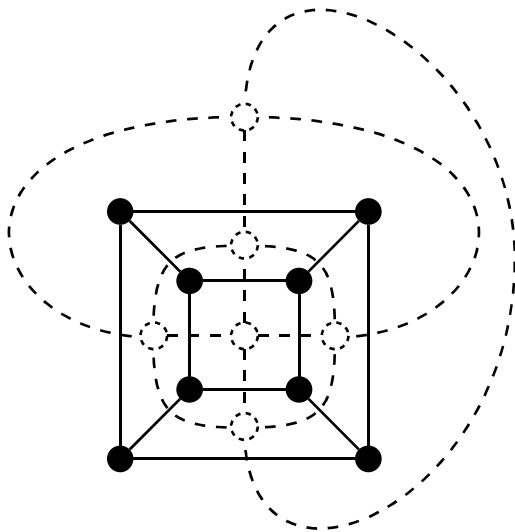
Till grafen $G = (V, E)$ bildas dess komplementgraf
 $\bar{G} = (V, E')$ så att $E \cap E' = \emptyset$, $K_n \cong (V, E \cup E')$, $(|V| = n)$,

det vill säga; det går kanter i \bar{G} mellan hörn x och y om det inte går en kant mellan dem i G .



Om ett hörn har valens δ i G , har det valens $(n - 1) - \delta$ i \bar{G} .

Den duala grafen G^\perp till en plan graf G beskriver grannrelationen för ytorna i G .



Hörnen i G^\perp svarar mot ytorna i G , en kant i G^\perp mot varje kant mellan ytorna.

Den duala grafen kan ha öglor, multipla kanter.

Heldraget:	G	hexaeder
Halvdraget:	G^\perp	oktaeder

$$(G^\perp)^\perp \cong G$$

Det kromatiska talet, $\chi(G)$ för G :

Minsta antalet färger som räcker för en hörnfärgning av G .

Exempel:

$$\chi(G) \leq |V|$$

$$\chi(G) = |V| \Leftrightarrow G = K_n, \text{ något } n.$$

$$\chi(G) = 2 \Leftrightarrow \text{Bipartit, } |E| \geq 1$$

$$\chi(G) = 1 \Leftrightarrow |E| = 0, |V| \geq 1$$

$$\chi(G) = 0 \Leftrightarrow |V| = 0$$

I allmänhet svårt att bestämma $\chi(G)$.

En girig algoritm (ger ofta ganska bra värden):

- 1) Ordna V : v_1, v_2, \dots, v_n $n = |V|$
- 2) Välj i tur och ordning $c(v_1) = 1, c(v_2), c(v_3), \dots$
minsta tillåtna värde (med hänsyn till redan färgade grannar).

Alla planära grafer kan hörnfärgas med 4 färger:

6-färgssatsen

5-färgssatsen

4-färgssatsen

Kromatiska polynomet för en graf $G = (V, E)$:

$P_G(\lambda)$ — antalet sätt att hörnfärga grafen G med λ färger.

Rekursion för att finna $P_G(\lambda)$:

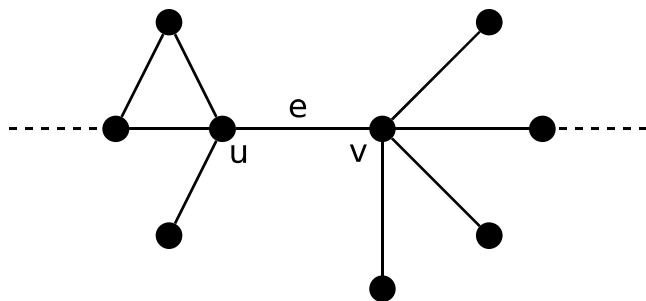
Låt $e \in E$ i $G = (V, E)$

Låt $G - e$: G med e borttagen
 G/e : G med e kontraherad

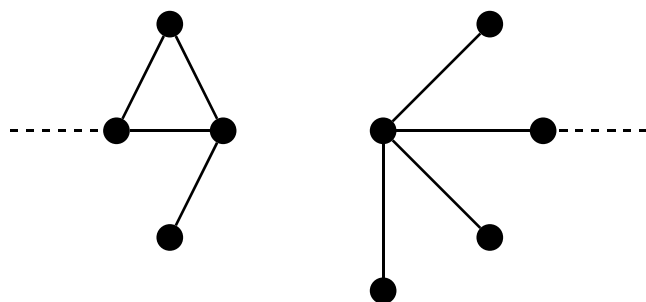
Då $P_{G-e}(\lambda) = P_G(\lambda) + P_{G/e}(\lambda)$ (additionsprincipen)

$P_{(V, \emptyset)}(\lambda) = \lambda^{|V|}$

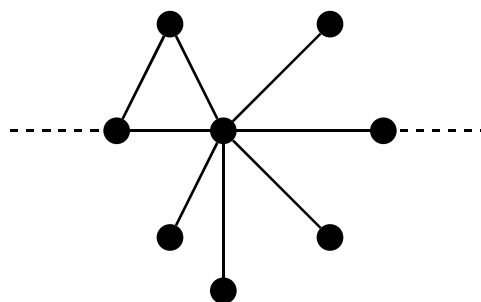
G :



$G - e$:



G/e :

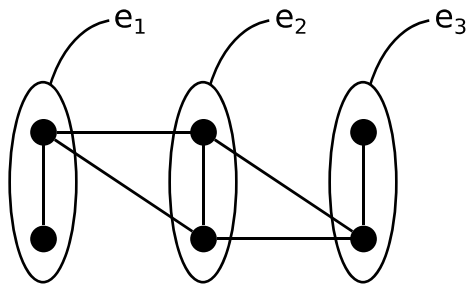


Med induktion (över antalet kanter) kan man visa:

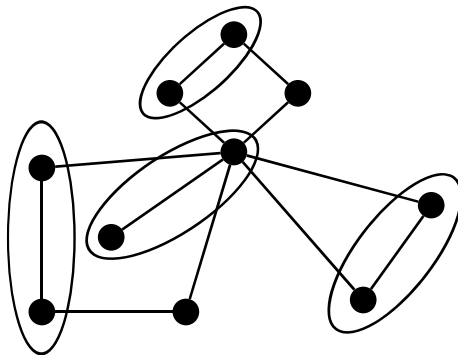
$$\left\{ \begin{array}{l} P_G(\lambda) \text{ är ett polynom i } \lambda. \\ \text{höstgradstermen: } \lambda^{|V|} \\ \text{nästgradstermen: } -|E|\lambda^{|V|-1} \\ \text{koefficienterna är heltal, alternerande } \geq 0, \leq 0. \end{array} \right.$$

Matchning i grafen $G = (V, E)$

↖
en delmängd M till E ($M \subseteq E$) med parvis disjunkta kanter ($\delta(v) \leq 1$).



Fullständig matchning, alla hörn ingår i en kant $M = \{e_1, e_2, e_3\}$.



Maximal matchning
 $|M|$ maximal

Vi talar här om matchning i bipartita grafer, $G = (X \sqcup Y, E)$.

För dem kallar vi en matchning fullständig om $|M| = |X| \leq |Y|$.

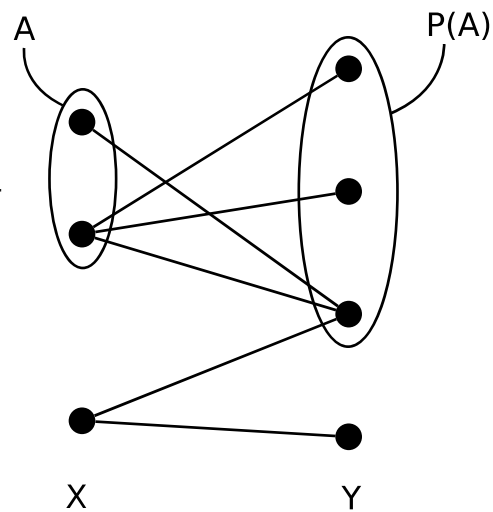
Halls sats: (giftermålssatsen)

En bipartit graf $G = (X \sqcup Y, E)$ har en fullständig matchning omm

$$|P(A)| \geq |A| \text{ för alla } A \subseteq X$$

där

$$P(A) = \{y \in Y \mid \{x, y\} \in E, \text{ något } x \in A\}$$



Sats:

En maximal matchning M av en bipartit graf har storlek $|M| = |X| - \delta(G)$

$$\delta(G) = \max_{A \subseteq X} \{|A| - |P(A)|\} \geq 0, \text{ G:s defekt (G:s underskott)}$$

Sats:

En matchning M i en bipartit graf G är maximal omm det inte finns en utökande alternerande stig för M i G . (Ger en algoritm för att finna maximal matchning.)

Övningsuppgift:

Om transversaler (så Halls sats formulerades först) (boken DMF sida 244) att finna "distinkta representanter" med $m_i \in M_i$ och $m_i \neq m_j$ om $i \neq j$. Finns de?

Halls sats säger att det går omm

$$\left| \bigcup_{i \in A} M_i \right| \geq |A| \text{ för alla } A \subseteq I, I \text{ ändlig.}$$

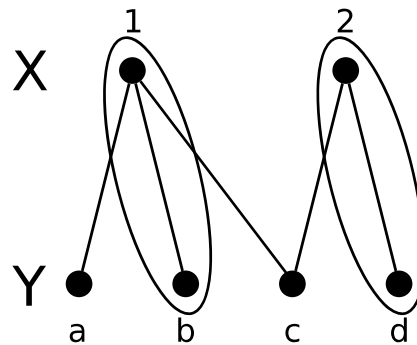
Ty:

Vi söker en fullständig matchning i en bipartit graf med

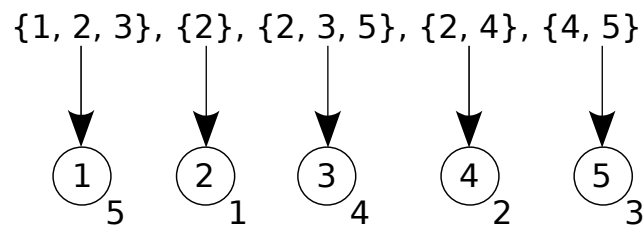
$$X = I, Y = \bigcup_{i \in I} M_i \quad \text{och}$$

kanter mellan $i \in I$ och alla element i M_i ,

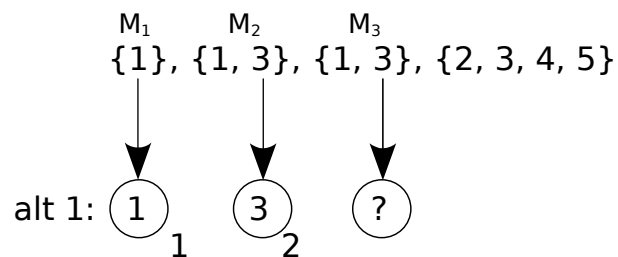
$$M_1 = \{a, b, c\}, \quad M_2 = \{c, d\}.$$



Vi söker en transversal till mängderna



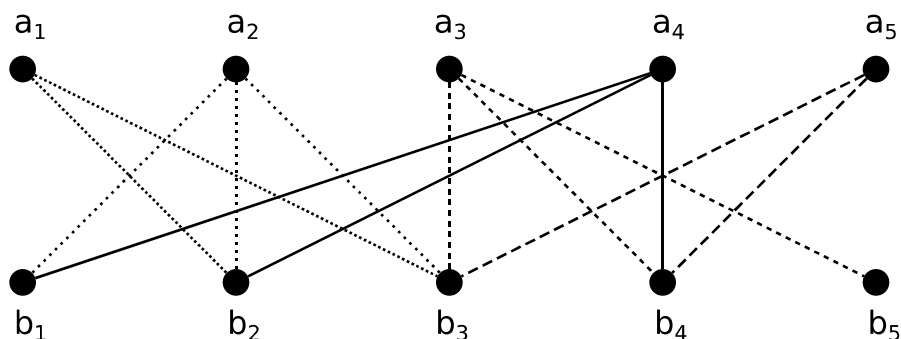
Varför finns ingen transversal till



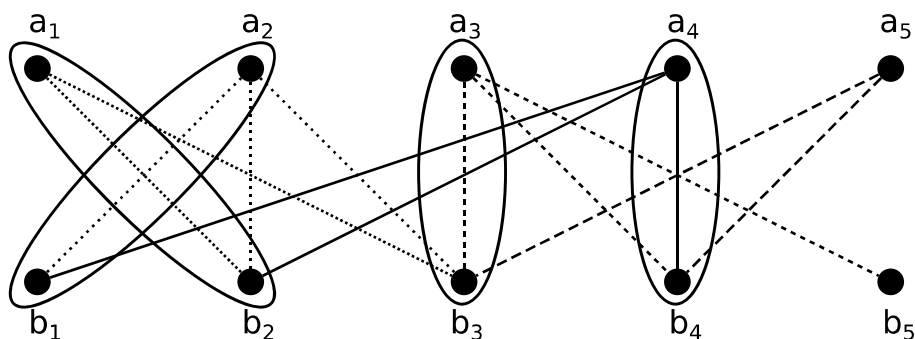
alt 2: Halls sats mängderna 1, 2, 3 har bara två element tillsammans, det vill säga färre element tillsammans än antalet mängder: ingen transversal.

Övningsuppgift:

Vi söker en fullständig matchningen till grafen



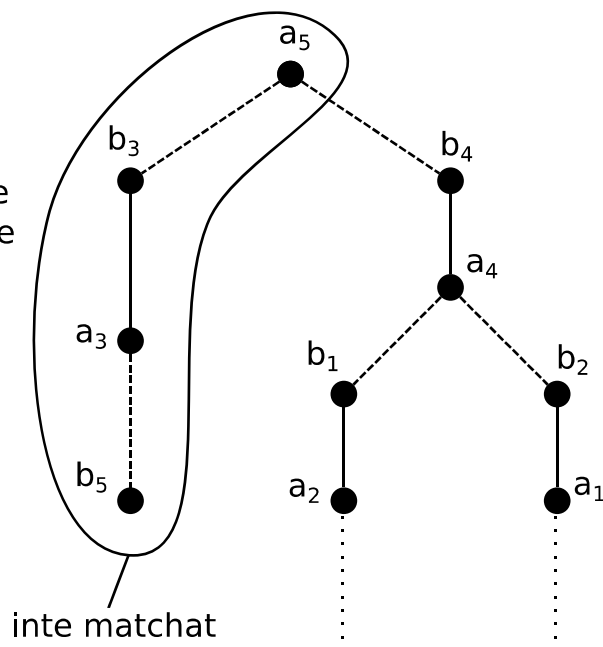
Efter 4 steg fås den ritade matchningen (nedan).
(Första lediga partiella matchningen tages, för varje a.)



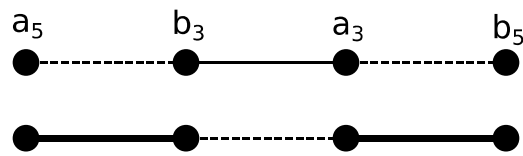
Hur skall a_5 matchas?

Sök en utökande alternerande stig!

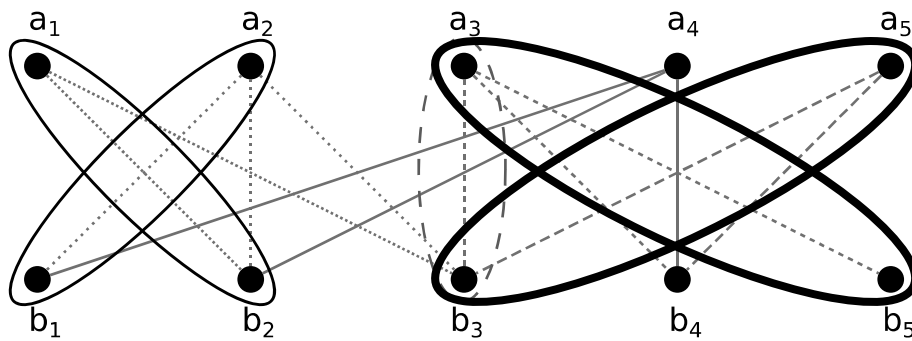
En utökande
alternerande
stig



Byt i den alternerande stigen.



Ger:



Övningsuppgift:

10 skrivande, 10 uppgifter.

Varje skrivande klarade minst 4 uppgifter.

Varje uppgift klarades av minst 5 skrivande.

A en mängd skrivande, $A \neq \emptyset$, $|P(A)| \geq 4$ (alla klarade minst 4)

Mängden uppgifter som någon i klarade.

$|A| > 4$ ger $|P(A)| = 10$

Varje uppgift klarades av ingen i A .

Så $|P(A)| \geq |A|$ för alla A — Halls sats...

Komplement

Komplementära ma. diskret-anteckningar

Den här sektion behandlar komplement till vår diskreta matematik, och är inte en del till kursen, men till av den kan till och med vara användbart på kursen.

Uttrycket
är logiskt ekvivalent med
men inte med

$$\begin{aligned} &\forall r \in \mathbb{R}, r > 0 \exists h \in \mathbb{R} : 0 < h < r \\ &\exists h \in \mathbb{R} \forall r \in \mathbb{R}, r > 0 : 0 < h < r \\ &\exists h \in \mathbb{R} : 0 < h < r \forall r \in \mathbb{R}, r > 0 \end{aligned}$$

Faktum är att det sista uttrycket ger en utvidning till de reella talen om man tar bort » $\in \mathbb{R}$ » i » $\exists h \in \mathbb{R}$ ». (eller ersätter \mathbb{R} , där i, med ${}^*\mathbb{R}$, de hyperreella talen).

Det hexadecimal talsystemet är består av siffrorna

0123456789 ABCDEF, men det är också vanligt med
0123456789 abcdef.

För används: 0123456789 0̇1̇2̇3̇4̇5̇

Det talsystem behöver inte vara naturligt (med naturliga tal som siffror), det finns även det negabinära talsystemet med -2 som bas (hexadecimal har 16). Man kan även ha imaginär, komplex &c bas. Det är faktiskt bara $|\beta| = 1$ och 0 samt hypertal (oändligheten, 1/oändligheten), där β är basen som är problematiskt.

RSA kryptering kan inte användas för att skicka meddelanden, det skulle ta för lång tid, dessutom måste man göra beräkningarna med en förbestämd till för att förhindra så kallad "time attack". Samt att RSA kryptering tappar sin säkerhet om icke-slumpmässiga meddelanden skickas.

RSA används bara för att skicka (slumpmässiga) nycklar till varandra. Dessa nycklar används då i ett symmetriskt krypto (i värsta fall Cæsarcipher).

Antalet ytor (område; fasetter) i en graf är en mer än antal cykler *omm* cyklerna är kantvis disjunkta, det vill säga har ingen gemensam kant. Om två cykler delar en kant så bildas en till cykel, utan att en yta bildas.

En ordentlig

Sammanfattning

Varning för intensivt oförklarat symbolspråk!
...och lite generallisering.

Sammanfattning, modul 1

$$p = qd + r, \quad 0 \leq r < |d|, \quad p, q, d, r \in \mathbb{Z}$$

p — det givna talet, täljare

q — kvot

d — divisor, $d \neq 0$; nämnare

r — rest

q och r finns entydligt.

x i basen t : $x = (r_n r_{n-1} \dots r_2 r_1 r_0)_t$

$r, q \in \mathbb{N}$, slutar vid (direkt efter) $q_n = 0$

$x = q_0 t + r_0$ start

upprepa:

$$q_{i+1} = q_i t + r_i$$

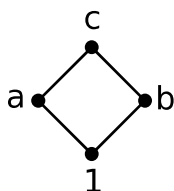
$$x = r_n t^n + r_{n-1} t^{n-1} + \dots + r_2 t^2 + r_1 t + r_0 = (r_n r_{n-1} \dots r_2 r_1 r_0)_t$$

Heltalsrelationen $d|m$ ($d|m$) innebär att $\exists q \in \mathbb{Z} : m = qd$.

$a \nmid a, a|a, 0|0, \pm 1|\pm 18, 0 \nmid a, \&c \quad b \neq 1, a \neq 0$

$$\text{sgd}(m, n) = \text{sgd}(n, m - qn)$$

Delargraf; med streck uppåt från direkt delare.



$$\Leftrightarrow \begin{array}{lll} 1|a, b; & a, b|c; & 1|c \text{ (indirekt);} \\ a \nmid b; & b \nmid a; & a, b \nmid 1; \quad c \nmid a, b, 1 \end{array}$$

$$d|a, d|b \Rightarrow d|(na + mb) \quad \forall m, n \in \mathbb{Z}$$

Euklides' algoritm:

$$q, r \in \mathbb{Z}; \quad a, b \in \mathbb{Z}$$

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$$r_{i-2} = q_i r_{i-1} + r_i$$

Stannar vid $r_n = 0$

$$\text{sgd}(a, b) = r_{n-1}$$

$$p \in \mathbb{P}, \quad p|ab \Rightarrow p|a \vee p|b$$

$$\text{sgd}(m, n) \cdot \text{mgm}(m, n) = m \cdot n$$

$$d|mn, \text{sgd}(d, m) = 1 \Rightarrow d|n$$

$$k|n, m|n \Rightarrow k|m$$

$$\text{mgm}(0, 0) = 0$$

Den diofantiska ekvationen (heltalslösningar sökes) $mx + ny = c$ har lösningar om $\text{sgd}(m, n) | c$.

$$\underbrace{x \equiv y \pmod{m}}_{x \equiv_m y} \stackrel{\text{def}}{\Leftrightarrow} m \mid (x - y)$$

I \mathbb{Z}_m är $x + y = (x + y) \bmod m$.

r i \mathbb{Z}_m är invertibel om

$$\exists x \in \mathbb{Z}_m : rx \equiv_m 1$$

$$x = r^{-1}$$

för \mathbb{Z}_p , $p \in \mathbb{P}$ är alla utom 0 invertibla.

$$\{\emptyset\} \neq \emptyset, \quad \{\emptyset\} \ni \emptyset, \quad \emptyset \not\ni \emptyset$$

$$|\emptyset| = 0, \quad |\{\emptyset\}| = 1$$

Mängdbyggning:

$$C = \{n : n \equiv_2 1\} = \{n \mid n \equiv_2 1\} = \{\text{udda heltal}\}$$

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

$$\mathbb{Z}_+ = \{1, 2, 3, \dots\}$$

$$\mathbb{N} = \{0, 1, 2, 3, \dots\} \text{ eller ibland } \{1, 2, 3, \dots\}$$

$$\mathbb{Q} = \{n \div m : m, n \in \mathbb{Z}, n \neq 0\}$$

$$\mathbb{R} = \{x : x \text{ reellt}\} \quad (\text{Omständigt att definiera.})$$

$$\mathbb{C} = \{x : x \text{ komplext}\} = \{x + yi : x, y \in \mathbb{R}, i^2 = -1\}$$

$$\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$$

$$A \cup B = \{x : x \in A \text{ eller } x \in B\}$$

$$A \cap B = \{x : x \in A \text{ och } x \in B\}$$

$$A \setminus B = \{x : x \in A \text{ och } x \notin B\}$$

$$A^c = \{x : x \notin A\} = \{x : x \notin A, x \in \mathcal{U}\}$$

\mathcal{U} — universum; mängden av alla möjliga element i fråga.

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

$$A \subseteq B \Rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$$

$$|A| < |\mathcal{P}(A)|$$

$$|\mathcal{P}(A)| = 2^{|A|}$$

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

$$|A \cap B| = 0 \text{ om } A \text{ och } B \text{ är disjunkta.}$$

$$A \times B = \{(a, b) : a \in A, b \in B\} \quad (a, b) \neq \{a, b\}$$

Induktionsbevis: (induktionsbevis skall inte förväxlas med Peanos' sista axiom)

För att visa ett påstående, P ,
 $P(n) \forall n \in X$ (ofta $X = \mathbb{N}$).

$\sigma(n)$ ger elementet efter n ; i \mathbb{N} : $\sigma(n) = n + 1$.
 $n_0 = 0$ i \mathbb{N} , det minsta elementet i X .

(Vi har bara behandlat induktionsbevis för \mathbb{N} .)

Bas: Visa att $P(n_0)$ är sant.

Steg: "Antag att påståendet är sant för n ".
Visa att $P(k)$ är sant för $k = \sigma(n)$.

"Alltså stämmer påståendet för att n ."

(Citat bör — tydligen — skrivas.)

Rekursion:

Symboler betyder samma sak som i induktionsbevis

Om $D_G = X \in \mathbb{N}$, $G(n, f)$, $f : X_n \rightarrow Y$, X_n är X till, men inte med, n .
så $\exists! f(n) : n \in X$.

Bas: $f(n_0)$ given.

Steg: $f(\sigma(k))$ bestäms av k och $f(k)$.

$\therefore f(n) = G(n, f) \geq n_0, \sigma(n_0), \sigma^2(n_0), \sigma^3(n_0), \dots, \sigma^{n-1}(n_0) \quad \sigma^{n-1}(n_0) = \sigma^{-1}(n)$

Injektion $f : x \mapsto y$ $f : X \hookrightarrow Y$

$$f(x) = f(y) \Rightarrow x = y$$

Eller ekvivalent (genom kontraposition):

$$x \neq y \Rightarrow f(x) \neq f(y)$$

Surjektion $f : x \rightarrow y$, $f : X \mapsto Y$ $f : X \twoheadrightarrow Y$

$$y \in Y \Rightarrow \exists x \in X : f(x) = y$$

Bijektion $f : x \rightarrow y$, $f : X \mapsto Y$ $f : X \leftrightarrow Y$, $f : X \twoheadrightarrow Y$, $f : X \hookrightarrow Y$

Injektion och surjektion

Eller ekvivalent:

$$\exists! \left(f^{-1} : \begin{matrix} X \rightarrow Y \\ x \mapsto y \end{matrix} \right) : \begin{cases} f^{-1}(f(x)) = x \quad \forall x \in X \\ f(f^{-1}(y)) = y \quad \forall y \in Y \end{cases}$$

$$|X| = \aleph_0 \Leftarrow \exists f : (f : \mathbb{N} \leftrightarrow X)$$

$$\exists f : (f : X \leftrightarrow Y) \Rightarrow |X| = |Y| \text{ om } |X| < \infty$$

$$|\mathbb{Q}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = \aleph_0 \neq |\mathbb{R}| = \beth_1$$

\aleph_0 — Uppräknerligt oändlig

\beth_1 — Överuppräknerligt oändlig

Binär relation:

$$\mathcal{R} = \{(a, b) \in X^2 : a \mathcal{R} b\} \subseteq X^2 (= X \times X) \quad (\text{Formell definition})$$

\mathcal{R} reflexiv: $x \mathcal{R} x \forall x \in X$

\mathcal{R} symmetrisk: $x \mathcal{R} y \Leftrightarrow y \mathcal{R} x \forall x, y \in X$

\mathcal{R} antisymmetrisk: $x \mathcal{R} y, y \mathcal{R} x \Rightarrow x = y \forall x, y \in X$

\mathcal{R} transitiv: $x \mathcal{R} y, y \mathcal{R} z \Rightarrow x \mathcal{R} z \forall x, y, z \in X$

Ekvivalensrelation om:

Reflexiv, symmetrisk och transitiv

Partialordning om:

Reflexiv, antisymmetrisk och transitiv

För $a \in X$:

Minimalt omm $x \leq a \Rightarrow x = a \forall x \in X$

Minst omm $a < x \forall x \in X, x \neq a$

a minst $\Rightarrow a$ minimalt

a minst $\nLeftarrow a$ minimalt

Exempel på Euklides' algoritm baklänges finns på sida 37
(2011-(02)feb-03: dag 6, 6).

Sammanfattning, modul 2

Additionsprincipen:

$$|\bigsqcup A_i| = \sum |A_i|$$

$$S \subseteq X, Y, \quad |X|, |Y| < \infty$$

$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} c_y(S)$$

$$r_x(S) = |\{y \in Y : (x, y) \in S\}|$$

$$c_y(S) = |\{x \in X : (x, y) \in S\}|$$

Multiplikationsprincipen:

$$S = X \times Y$$

$$|S| = |X| \cdot |Y|$$

$$\therefore |X \times Y| = |X| \cdot |Y|$$

Vid likafördelning: (Allt är lika sannolikt)

$$P(A) = \frac{|A|}{|\Omega|}$$

$P(A)$ — Sannolikheten för att A inträffar

A — Händelse; mängd av elementarhändelser

Ω — Utfallsrum; alla elementarhändelser (utfall)

$$A \subseteq \Omega$$

A, B oberoende om:

$$P(A \cap B) = P(A) \cdot P(B)$$

$$(P(A \cap B) = P(A) \cdot P(B))$$

$$P(A \sqcup B) = P(A) + P(B)$$

Om $|X| = m < \infty$, $|Y| = m < \infty$:

$$|\{f \mid f: X \rightarrow Y\}| = n^m = |Y^m| = |\{\text{ord } x : x\text{'s längd} = m, \text{ alfabet} = Y\}| = |\{\text{ordnade val av } m \text{ stycken ur } Y \text{ med upprepning}\}|$$

”Ordnat val med upprepning”

Om $|X| = m < \infty$, $|Y| = m < \infty$:

$$\begin{aligned} |\{f \mid f: X \hookrightarrow Y\}| &= |\{\text{ord av längden } m, \text{ alfabet } Y, \text{ ingen återanvändning av bokstäver}\}| = |\{\text{ord, ordnade val av } m \text{ stycken ur } Y \text{ utan upprepning}\}| = \\ &= \prod_{i=0}^{m-1} (n - i) = (m)_n = \frac{n!}{(n - m)!} \end{aligned}$$

”Ordnat val utan upprepning”

Om $m = n$:

Antalet = $n!$ (Antalet permutationer för en n -mängd.)

Oordnat urval utan upprepning, $|X| = n < \infty$:

Binomialtalet $\binom{n}{k}$ — k stycken ur X .

(Det är viktigt att rundparenteser används för att inte förväxlas med Stirlingtalen.)

Multinomialtal

$$\binom{n}{k_1, k_2, \dots, k_m} = \frac{n!}{k_1! k_2! \dots k_m!}, \quad k_i \geq 0, \sum k_i = n \qquad \binom{n}{k} = \binom{n}{k, n - k}$$

Antalet sätt att dela in n stycken i m grupper med olika storlekar k på grupperna.

Oordnat val med upprepning:

Antalet sätt att skriva

$$k = x_1 + x_2 + \dots + x_n \quad x_i \geq 0$$

$$\text{är } \binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

Postfacksprincipen: (duvslagsprincipen, en. pigeonhole principle)

$$|X| > |Y| \Rightarrow \nexists f : X \hookrightarrow Y$$

(Gäller även oändliga mängder.)

$$S_n = \{f \mid f : X \hookrightarrow Y, X = \{1, 2, 3, \dots, n\}\}$$

Stirlingtal (av andra slaget):

$S(n, k)$ = antalet sätt att gruppera n särskiljbara element i k icke-tomma särskiljbara grupper.

$$\begin{cases} S(n, k) = S(n-1, k-1) + k \cdot S(n-1, k) & 1 < k < n \\ S(n, 1) = S(n, n) - 1 & n \geq 1 \end{cases}$$

Antalet surjektioner $f : X \rightarrow Y$ är $k! \cdot S(n, k)$,

där $|X| = n$, $|Y| = k$.

Sammanfattning, modul 3

$(G, *)$ (oftare skrivet $\langle G, * \rangle$) är en grupp om:

Slutenhet:

$$x * y \in G \quad \forall x, y \in G$$

Associativitet:

$$(x * y) * z = x * (y * z) \quad \forall x, y, z \in G$$

Identitetselement: (enhetsselement)

$$\exists I \in G : I * x = x * I = x \quad \forall x, y \in G$$

Invers: (där I är som ovan)

$$\forall x \in G \exists x^{-1} \in G : x * x^{-1} = x^{-1} * x = I$$

Kommutativitet är inte ett krav.

$*$ skrivs sällan ut.

$(G, *)$ kallas abelsk eller kommutativ om:

$$a * b = b * a \quad \forall a, b \in G$$

(+ brukar användas om en grupp är abelsk.)

Grupptabeller (till exempel multiplikationstabeller) är latinska kvadrater:

$$ax = ay \Rightarrow x = y \Leftarrow xa = ya$$

$$|G| = p^2, p \in \mathbb{P} \Rightarrow G \text{ abelsk}$$

$|G|$ — G :s ordning

$g \in G$ har ordningen $o(g)$, $o(g)$ är det minsta $n > 0$ sådant att $g^n = 1$, 1 är G 's identitets-element (gäller alltid härifrån).

$o(g) = \infty$ om inget sådant finns.

$$o(g) = m, g^s = 1 \Rightarrow m \mid s$$

G kallas cyklisk om:

$$\exists g : \forall x \in G \exists n \in \mathbb{Z} : x^n \in G$$

då: $G = \langle g \rangle$, g är G 's generator, det genererande elementet.

Om $o(g) = m$:

$$G = \{1, g, g^2, g^3, \dots, g^{m-1}\}$$

Om $o(g) = \infty$:

$$G = \{\dots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, \dots\}$$

G 's centrum:

$$Z(G) = \{z \in G : zg = gz \forall g \in G\}$$

G 's centralisator:

$$C(g) = \{x \in G : xg = gx \forall g \in G\}$$

$$Z(G) = \bigcap_{g \in G} C(g), \quad g \in Z(G) \Rightarrow C(g) = G$$

Sidoklasser: (även kallat restklasser) (en. cosets)

H delgrupp till G , $g \in G \Rightarrow gH = \{gh : h \in H\}$.
 H är en vänstersidoklass.

(Om $|H| < \infty$ så) $|H| = |gH| = |Hg|$

Lagranges sats:

$$|G| < \infty, H \subseteq G, \text{ grupper} \Rightarrow |H| \mid |G|$$

H 's index i G (antalet sidoklasser)

$$|G : H| = \frac{|G|}{|H|} \quad |G : H| \text{ skrivs även } [G : H]$$

$$|G|, |H| < \infty$$

$|G| < \infty$, G grupp, $g \in G \Rightarrow o(g) \mid |G|$ och $g^{|G|} = 1$

$|G| = p \in \mathbb{P}$, G grupp $\Rightarrow G$ cyklisk

En gruppisomorfi mellan två grupper, (G_1, \bullet) och (G_2, \circ) ,
är en bijektion $\phi : G_1 \rightarrow G_2$ sådan att:

$$\phi(a \bullet b) = \phi(a) \circ \phi(b)$$

$$(G_1, \bullet) \cong (G_2, \circ)$$

En ekvivalensrelation.

Permutation π

$$\pi = [\text{cabedf}] = \underbrace{\begin{pmatrix} a & b & c & d & e & f \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ c & a & b & e & d & f \end{pmatrix}}_{\text{Tvåradnotation}} = \underbrace{\begin{pmatrix} a & b & c & d & e & f \\ c & a & b & e & d & f \end{pmatrix}}_{\text{Enradsnotation}} = \underbrace{(a \ c \ b)(d \ e)(f)}_{\text{Cykelnotation}} = \underbrace{(a \ c \ b)(d \ e)}_{\text{Reducerad cykelnotation}}$$

Cayleys sats:

$$G \text{ grupp} \Rightarrow \exists G^* \subseteq S_G : G \cong G^*$$

S_G — Permutationer av G

Om π i cykelnotation är: $\underbrace{(\alpha \ \beta \ \gamma \ \delta)}_{\pi\text{:s cykelstruktur}} \underbrace{(a \ b \ c)}_{m=4} \underbrace{(A \ B \ C)}_{n=3} \underbrace{}_{k=3}$

så är $o(\pi) = \text{lcm}(m, n, k) = 12$;

$$m, n, k \mid o(\pi)$$

Konjugering i S_n (en ekvivalensrelation):

$\alpha, \beta \in S_n$ är konjugerade om

$$\exists \sigma \in S_n : \underbrace{\sigma \alpha \sigma^{-1}}_{\sigma \alpha = \beta \sigma} = \beta$$

Santa om de har samma cykelstruktur.

En grövre uppdelning av S_n :

Jämna och udda permutationer

En transposition: Permutation av typen $[1^{n-2} 2]$, det vill säga $(i j)$, $i \neq j$.

$\pi \in S_n$:s cykelstruktur kan skrivas som en serie sådana:

$$\pi = \tau_r \tau_{r-1} \cdots \tau_2 \tau_1$$

π är jämn/udda när r är jämn/udda.

$$\operatorname{sgn} \pi = (-1)^r$$

Om $\pi \in S_n$, $\pi = \tau_r \cdots \tau_1 = \tau'_r \cdots \tau'_1$
så har r och r' samma paritet, de är båda jämna eller båda udda.

$$\operatorname{sgn} \pi\sigma = \operatorname{sgn} \pi \cdot \operatorname{sgn} \sigma$$

$$\operatorname{sgn} \pi^{-1} = \operatorname{sgn} \pi$$

$$\operatorname{sgn} \sigma\alpha\sigma^{-1} = \operatorname{sgn} \alpha$$

I S_n , $n \geq 2$, är hälften av permutationerna jämna och hälften udda.

Determinanter:

$$\det_{a \times a} A = \sum_{\pi \in S_n} \operatorname{sgn} \pi \prod_{i=1}^n a_{\pi(i)i}$$

En ring $(R, +, \cdot)$ är en kommutativ grupp $(R, +)$ med identitetslement 0, och en grupp (R, \cdot) med identitetslement 1, där \cdot är distributiv med avseende på $+$.
 $(F, +, \cdot)$ är en kropp (en. field) om dessutom $(F \setminus \{0\}, \cdot)$ är en kommutativ grupp.

Sammanfattning, modul 4

En binär felrättande kod $\mathcal{C} \subseteq \mathbb{Z}_2^n$, där n är kodens längd.

$$\mathbb{Z}_2^n = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

Element i \mathcal{C} är egentligen vektorer.

$$\mathbb{Z}_2:$$

+	0	1
0	0	1
1	1	0

Viktiga egenskaper hos \mathcal{C} :

Hur många fel som säkert kan:

upptäckas
hittas.

\mathcal{C} kan upptäcka $\delta - 1$ fel och rätta $\left\lfloor \frac{\delta - 1}{2} \right\rfloor$ fel.

(Och återskapa $\delta - 1$ döda (försvunna med känd position) bitar)

Där δ är det minimala avståndet för \mathcal{C} :

$$\delta = \min\{\partial(a, b) : a, b \in \mathcal{C}, a \neq b\}$$

$$\partial(a, b) = \sum_{i=1}^n a_i \oplus b_i \quad (\text{antalet positioner, } i, \text{ där } a_i \neq b_i)$$

\swarrow
 \downarrow
 \downarrow

$+ i \mathbb{Z}_2$
 $+ i \mathbb{Z}$

Sfärpackningssatsen:

$$|\mathcal{C}| \left(\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{e} \right) \leq 2^n$$

Där n är \mathcal{C} 's längd och e är antalet fel \mathcal{C} säkert rättar.
Likhet för Hammingkoder; en perfekt kod.

\mathcal{C} är en linjär kod omm:

$$a, b \in \mathcal{C} \Rightarrow a + b \in \mathcal{C}$$

Då: $|\mathcal{C}| \mid 2^n \therefore |\mathcal{C}| = 2^k, \mathbb{N} \ni k = \mathcal{C}$:s dimension

$$\delta = \omega_{\min} = \min\{\omega(c) : c \in \mathcal{C}, c \neq \vec{0}\}$$

$$\omega(c) = c\text{:s vikt} = \text{antalet } 1\text{:or i } c = \sum_{i=1}^n c_i$$

(Paritets)kontrollmatris:

\mathbf{H} , en $m \times n$ 0/1-matris, har en tillhörande linjär kod
 $\mathcal{C} = \{x \in \mathbb{Z}_2^n : \mathbf{H}x = \vec{0}\}$, med dimension $n - \text{rank } \mathbf{H}$.

Om \mathbf{H} :s alla kolonner är olika och skilda från $\vec{0}$,
så rättar \mathbf{H} säkert ett fel.

För sådana koder gäller:

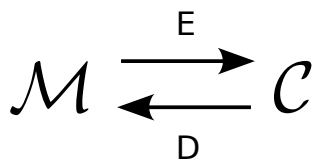
$$\mathbf{H}z = \begin{cases} \vec{0} & \text{om inget fel hittats} \\ \mathbf{H}\text{:s } i\text{:te kolonn, där } i \text{ är biten som är fel} \end{cases}$$

$\mathbf{H}z = (\text{XOR-})\text{summan av all fel.}$

z — Det mottagna meddelandet

Vid för många fel kan det hända att rättningen inte ger ett korrekt kodord, men med rätt paritet.

(Asymmetrisk) kryptering:



\mathcal{M} — Meddelande
 \mathcal{C} — Chiffer

E — Kryptering
 D — Dekryptering

$$D = E^{-1}$$

E :s nyckel är känd, men så komplicerad att det är svårt(!) att bestämma D :s nyckel; en envägsfunktion.

RSA (Rivest, Shamir, Adleman) är ett sådant krypto (det mest kända, och mest använda), och grundar sig på Fermats lilla sats.

Fermats lilla sats:

$$a^{p-1} \equiv 1 \pmod{p}, a \neq 0, p \in \mathbb{P}$$

($a^p \equiv_p 1$ är en generalisering, som inte bara gäller $a \neq 0, p \in \mathbb{P}$)

$$p \nmid a \Rightarrow p \mid a^{p-1} - 1$$

$$p \mid a^p - a \quad \forall a \in \mathbb{Z}$$

Om $p, q \in \mathbb{P}$:

$$n = pq, \quad m = (p-1)(q-1)$$

$$x^s \equiv 1 \pmod{m} \Rightarrow x^s \equiv x \pmod{n} \quad \forall x \in \mathbb{Z}$$

RSA:

Välj $p, q \in \mathbb{P}$, $p, q \gtrsim 10^{150}$

$$n = pq, \quad m = (p - 1)(q - 1)$$

Välj $e : \text{sgd}(e, m) = 1$

Finn $d : ed \equiv 1 \pmod{m}$ (med Euklides' algoritm)

Offentliggör n och e , men hemlighåll d (och kasta (hemlig) m).

$$\begin{array}{ll} E(x) = x^e \bmod n & E : \mathbb{Z}_n \rightarrow \mathbb{Z}_n \\ D(x) = x^d \bmod n & D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n \end{array}$$

Elektronisk signatur:

B skickar till A:

$$E_A(D_B(x)) \quad \text{eller} \quad D_B(E_A(x))$$

När A läser signaturen:

$$D_A(E_A(D_B(x))) = D_B(x)$$

$$E_B(D_B(x)) = x \quad E_B \text{ är offentlig}$$

Primalitetstest:

Pröva faktorer ($\sqrt{n} \approx 10^{75}$, $n \approx 10^{150}$)

Fermats lilla sats!

Fermattestet: Med bas b för primalitet hos.

$$\text{Är } b^{N-1} \equiv 1 \pmod{N}?$$

Endast om, men inte om, ja, så primtal.

Pseudoprimtal är icke-primtal (sammansatta tal) som klarar test.

Carmichaeltal är problematiska för Fermaltestet:

Finns oändligt många.

Klarar alla Fermattest med bas b : $\text{sgd}(b, N) = 1$.

N är ett Carmichaeltal omm:

kvadratfritt och
 $p \mid N \Rightarrow p - 1 \mid N - 1$

Ett starkare test; Miller-Rabins test:

En förfinning av Fermattestet

$N - 1 = n \cdot 2^r$, n udda, $r \geq 1$ (N udda)

$b^n \pmod{N}$

$(b^n)^2 \pmod{N}$

$((b^n)^2)^2 \pmod{N}$

\vdots

$b^{n \cdot 2^r} \equiv 1 \pmod{N}$

Endast om, men inte om, $b^n \equiv_N 1$ eller $(b^n)^{2^i} \equiv_N -1$,
något i , $0 \leq i < r$, så är N ett primtal.

1 = sant, 0 = falskt

Konnektiv:

Negation: $\neg 1 = 0$ (inte)
 $\neg 0 = 1$

Konjunktion: $1 \wedge 1 = 1$ (och)
 $1 \wedge 0 = 0$
 $0 \wedge 1 = 0$
 $0 \wedge 0 = 0$

Disjunktion: $1 \vee 1 = 1$ (eller)
 $1 \vee 0 = 1$
 $0 \vee 1 = 1$
 $0 \vee 0 = 0$

Implikation: $1 \rightarrow 1 = 1$ (om ... så ...)
 $1 \rightarrow 0 = 0$
 $0 \rightarrow 1 = 1$
 $0 \rightarrow 0 = 1$

Dubble implikation: $1 \leftrightarrow 1 = 1$ (om och endast om)
 $1 \leftrightarrow 0 = 0$
 $0 \leftrightarrow 1 = 0$
 $0 \leftrightarrow 0 = 1$

$p \rightarrow q \equiv \neg q \rightarrow \neg p$ (kontraposition)

$p \rightarrow q \not\equiv q \rightarrow p$ (omvändning)

\equiv betyder att uttrycken (de sammansatta konnektiven) är ekvivalenta.

\top : alltid falsk (falsum)

\perp : alltid sann (verum)

0-ställiga konnektiv:	\top	\perp		
1-ställiga konnektiv:	\neg			
2-ställiga konnektiv:	\wedge	\vee	\rightarrow	\leftrightarrow

Boolesk algebra

Regel:	Ett skrivsätt:	(xy kan också skrivas $x \cdot y$) Ett annat skrivsätt:
Kommutativitet:	$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$	$pq = qp$ $p + q = q + p$
Associativitet:	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(pq)r = p(qr)$ $(p + q) + r = p + (q + r)$
Distributivitet:	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p(q + r) = pq + pr$ $p + qr = (p + q)(p + r)$
De Morgan:	$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\overline{pq} = \overline{p} + \overline{q}$ $\overline{p + q} = \overline{p} \overline{q}$
Idempotens:	$p \wedge p \equiv p$ $p \vee p \equiv p$	$pp = p$ $p + p = p$
Absorption:	$p \wedge (p \vee q) \equiv p$ $p \vee (p \wedge q) \equiv p$	$p(p + q) = p$ $p + pq = p$
Involution:	$\neg\neg p \equiv p$	$\overline{\overline{p}} = p$
\leftrightarrow uttryckt. \rightarrow uttryckt: \neg uttryckt:	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ $p \rightarrow q \equiv \neg p \vee q$ $\neg p \equiv p \rightarrow \perp$	$\rightarrow, \leftrightarrow$ saknas i denna notation
Komplitaritet:	$p \wedge \neg p \equiv \perp$ $p \wedge \perp \equiv \perp$ $p \wedge \top \equiv p$	$p\overline{p} = \mathbf{0}$ $p\mathbf{0} = \mathbf{0}$ $p\mathbf{1} = p$

Motsvarighet med mängdlära:

$$\begin{array}{ll}
 A \cap B & \equiv p \wedge q \\
 A \cup B & \equiv p \vee q \\
 A^c & \equiv \neg p \\
 \emptyset & \equiv \perp \\
 \mathcal{U} & \equiv \top
 \end{array}$$

Samma regler gäller.

I boolesk algebra: $\mathbb{B}_n = \{0, 1\}^n = \{ \underbrace{00\dots 0}_{x_n}, 00\dots 1, \dots, 11\dots 1 \}$

\mathbb{B} :	$+$	0	1	\cdot	0	1
	0	0	1	0	0	0
	1	1	1	1	0	1

inte som i \mathbb{Z}_2

Disjunktiv normalform (dnf):

$$f(\vec{x}) = \sum_{f(\vec{x})=1} \prod_{i=1}^n x_i \quad \text{där } n \text{ är antalet element i } \vec{x}.$$

Det vill säga:

Omm $f(\vec{x}) = 1$ så är p en term i $f(\vec{x})$ där p är produkten av alla element $x \in \vec{x}$, där x inverteras omm $f(\vec{x}) = 1$ om det x :et = 0.

Till exempel:

	x	y	z	$f(x, y, z)$	
	1	1	1	1	xyz
	1	1	0	1	$xy\bar{z}$
	1	0	1	1	$x\bar{y}z$
(1)	1	0	0	0	
(2)	0	1	1	0	
(3)	0	1	0	0	
	0	0	1	1	$\bar{x}\bar{y}z$
(4)	0	0	0	0	

$$f(x, y, z) = xyz + xy\bar{z} + x\bar{y}z + \bar{x}\bar{y}z$$

Dualt: Konjunktiv normalform (knf):

$$f(x, y, z) = (\underbrace{\bar{x} + y + z}_{(1)})(\underbrace{x + \bar{y} + \bar{z}}_{(2)})(\underbrace{x + \bar{y} + z}_{(3)})(\underbrace{x + y + z}_{(4)})$$

Karnaugh-diagram kan användas för att finna en (eller flera) minimal disjunktiv form. (Detta behöver inte ge en minimal form, bara minimal disjunktiv form.)

Rita en rektangel (eller för fler än 4 variabler, en kub, tesseract, ...), med sidor av storlekerna 2 eller 4.

Om en sida motsvarar en variable, a , så är den sidan av storlek 2, och dess två positioner motsvarar \bar{a} respektive a .

Om en sida motsvarar två variabler, a och b , så är den sidan av storlek 4, och dess fyra positioner motsvarar $\bar{a}\bar{b}$, $\bar{a}b$, ab respektive $a\bar{b}$ (en skillnad per steg).

Fyll i f 's värde för varje position.

Ringa sedan in 1:orna med så stora, och få, ringa som möjligt, av sidor med storlek 2^n . Man får gå från en kant till motstående kant.

Ringar motsvarar nu varje term i f 's minimala disjunktivform.

Till exempel: f :

		\bar{z}	z
		0	1
\bar{y}	\bar{x}	0 0	0 1
	x	0 1	0 0
	\bar{y}	1 1	1 1
	y	1 0	0 1

$$f(x, y, z) = \underline{\bar{x}y} + \underline{\bar{y}z}$$

Logisk kretsar har logiska grindar:

$$\begin{array}{c} a \\ b \end{array} \begin{array}{|c|} \hline \& \\ \hline \end{array} \begin{array}{c} \text{---} c \end{array} \quad \equiv \quad c = a \wedge b = a \cdot b$$

$$\begin{array}{c} a \\ b \end{array} \begin{array}{|c|} \hline \geq 1 \\ \hline \end{array} \begin{array}{c} \text{---} c \end{array} \quad \equiv \quad c = a \vee b = a + b$$

$$\begin{array}{c} a \\ b \end{array} \begin{array}{|c|} \hline 1 \\ \hline \end{array} \begin{array}{c} \text{---} c \end{array} \quad \equiv \quad c = \neg a = \bar{a}$$

ringen inverterar

Sammanfattning, modul 5

En graf, $G = (V, E)$, består av hörn, V , och kanter, E . Mellan två hörn och endast mellan två hörn, $v_1, v_2 \in V$, kan det finnas en kant $\{v_1, v_2\} \in E$, v_1 och v_2 kallas isåfall grannhörn.

En graf kan vara:

oändlig	$ V = \infty$
riktad	$v_1 \rightarrow v_2, v_1 \nleftrightarrow v_2$
viktad	$v_1 \xrightarrow{\omega} v_2$

eller ha:

icke-enkel $\left\{ \begin{array}{ll} \text{öglor} & v_1 \text{ --- } v_1 \\ \text{multipla kanter} & v_1 \text{ --- } v_2 \end{array} \right.$

Vi behandlar nästan exklusivt enkla, ändliga, oriktade, oviktade grafer.

Standard grafer:

Fullständig grafer — $K_n = (V, \{uv : u, v \in V, u \neq v\}), |V| = n \geq 1$

Cykliska grafer — $C_n = (\{v_i : 0 \leq i < n\}, \{v_i v_j : j \equiv i + 1\}), n \geq 3$

Fullständiga bipartita grafen — $K_{m,n} = (A \sqcup B, \underbrace{\{ab : a \in A, b \in B\}}_{A \times B}), |A| = m \geq 1, |B| = n \geq 1$

Grannlista

a	b	c	...
α	β	γ	\vdots
\vdots	\vdots	\vdots	

Alla hörn som a går till.

Grannmatris

$$A_{n \times n} = [a]_{ij} = \underbrace{[\text{antal kanter från } v_i \text{ till } v_j]}_{(\text{Öglor räknas dubbelt})}_{ij}$$

$$n = |V|, \quad v \cong V$$

Incidentmatris

$$A_{n \times m} = [a]_{ij}, \quad a_{ij} = \begin{cases} 1 & \text{om } v_i \in e_j \\ 0 & \text{annars} \end{cases}$$

$$\begin{aligned} n &= |V|, & v &\cong V \\ m &= |E|, & e &\cong E \end{aligned}$$

$G_1 \cong G_2$ betyder att graferna G_1 och G_2 är isomorfa, det vill säga:

$$\exists (\phi : V_1 \leftrightarrow V_2) : (\{x, y\} \in E_1 \Leftrightarrow \{\phi(x), \phi(y)\} \in E_2)$$

$$G_1 = (V_1, E_1)$$

$$G_2 = (V_2, E_2)$$

Valens:

$\delta(v)$ = antalet kanter från v (öglor räknas dubbelt)

En graf kallas n -reguljär om:

$$\delta(v) = n \quad \forall v \in V$$

K_n är $(n - 1)$ -reguljär

C_n är 2-reguljär

$$\sum_{v \in V} \delta(v) = 2|E|$$

Antalet udda hörn (hörn med udda valens) är alltid jämt.

Kantföljder:

Vandring:	Mellan grannhörn
Väg:	Vandring utan kantupprepning
Krets:	Sluten väg
Stig:	Väg utan hörnupprepning
Cykel:	Sluten stig

En grafs komponenter är grafens maximala sammanhängande delgrafer.

En Eulerväg är en väg som passerar varje kant exakt en gång. En graf har en Eulerväg om den är sammanhängande och har högst 2 udda hörn.

Den har en Eulerkrets om dessutom alla hörn är jämna.

Man kan sätta ihop en Eulerväg/-krets med flera Eulerkretsar.

En Hamiltonstig/-cykel passerar varje hörn exakt en gång.

Ett träd är en sammanhängande, acklisk graf, betecknas ofta $T = (V, E)$.
Om ingenting(!) sägs brukar T beteckna ett linjärt träd.

En graf där alla komponenter är träd, det vill säga en acyklisk graf, kallas en skog.

I ett träd finns en unik stig mellan två godtyckliga hörn, och $|E| = |V| - 1$.

I varje sammanhängande graf finns minst ett träd,
ett (upp)spännande träd, sådant att:

$$T = (V, E'), \quad E' \subseteq E \quad \text{där } G = (V, E)$$

Kruskals algoritm är en girig algoritm som kan användas för att finna ett minimalt spännande träd för en graf, ett spännande träd med minimal summa av kantvikter (grafen är viktad):

För varje steg lägg till den lättaste kanten som inte bildar en cykel.

Rotade binära träd är viktiga för datalagring. De har ett hörn som kallas rot, och saknar föräldrar. Föräldrar (varje hörn utom roten har exakt en förälder) ritas ovanför dess barn. Varje hlrn har max två barn, ett vänsterbarn med lägre tillhörande värde, och ett högerbarn med högre tillhörande värde.

En planär graf är en graf som är isomorf med en plan graf, en graf ritad på ett plan *eller på en sfär* utan korsade kanter.

K_4 , men inte K_5 och $K_{3,3}$, är en sådan.

De minimala cyklerna i en plan graf bildar ytor,
dessutom finns en (på ett plan) obegränsad yta.

Generallisering av Eulers polyederformel:

$$v - e + r - c = 1$$

v — antalet hörn

e — antalet kanter

r — antalet ytor

c — antalet komponenter

Gäller för plana grafer.

Krav för planaritet:

$$3v \geq e + 6$$

Komplementgraf:

$$\overline{G} = (V, E'), \quad E' \cap E = \emptyset$$

är en komplementgraf till $G = (V, E)$.

$$K_n \cong (V, E \cup E'), \quad n = |V|$$

\overline{G} är sammanhängande om G är osammanhängande.

$$\delta'_i = n - 1 - \delta_i$$

Dualgraf: G är plan

G^\perp :s hörn svarar mot G :s ytor.

G^\perp :s kanter svarar mot kanter mellan ytor i G .

G^\perp kan ha öglor och multipla kanter.

$$(G^\perp)^\perp \cong G$$

Vi går inte in på kantfärgning, däremot kommer resten nu handla om hörnfärgning, förutom lite matchning i slutet.

$$c : V \rightarrow \mathbb{N}$$

$$\{x, y\} \in E \Rightarrow c(x) \neq c(y)$$

Det kromatiska talet $\chi(G)$ för en graf, G , är hur många färger som räcker (minsta antalet) för att färga G .

$$\chi(G) \leq |V|$$

$$\chi(G) = |V| \Leftrightarrow G = K_n$$

$$\chi(G) = 2 \Leftrightarrow G \text{ bipartit med kanter}$$

$$\chi(G) = 1 \Leftrightarrow G \text{ saknar kanter, men har hörn}$$

$$\chi(G) = 0 \Leftrightarrow G \text{ saknar hörn}$$

6-, 5- och färgssatserna säger att om en graf, G , är planär så är $\chi(G) \leq 6, 5$ respektive 4.

Så om G är planär så är $\chi(G) \leq 4$, vilket gör det lätt att bestämma $\chi(G)$ för planära grafer, annars är det ofta svårt.

En girig algoritm för att finna ett maximalt värde på $\chi(G)$, som ofta ger ett ganska bra resultat, det vill säga nära $\chi(G)$:

- 1) Ordna V : $v_1, v_2, v_3, \dots, v_n, \quad n = |V|$
- 2) Välj i tur och ordning $c(v_i)$, $c(v_1) = 1$, med hänsyn till redan färgade grannar.

$$\chi(G) \leq \delta_{\max} + 1$$

$$\chi(G) \leq \delta_{\max} \text{ om sammanhängande och inte reguljär.}$$

Det kromatiska polynomet för en graf G :

$P_G(\lambda)$ — Antalet sätt att färga grafen G med λ färger.

$$P_T(\lambda) = \lambda(\lambda - 1)^{n-1}, |V| = n$$

något träd $T = (V, E)$

Rekursion för att finna $P_G(\lambda)$:

$$e \in E, G = (V, E)$$

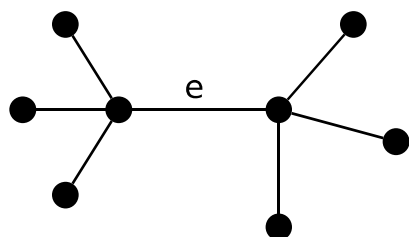
$$P_{(V, \emptyset)}(\lambda) = \lambda^{|V|}$$

$$P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda)$$

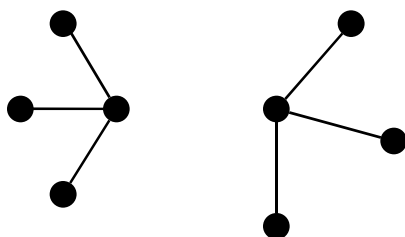
$G - e$: G med e borttagen

G/e : G med e kontraherad (ihopdragen)

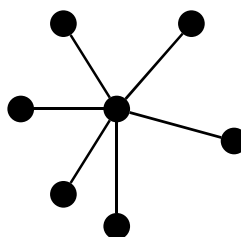
G :



$G - e$:



G/e :



En matchningen, M , i grafen $G = (V, E)$, är en delmängd till E ($M \subseteq E$) sådan att kanterna är parvis disjunta ($\delta(v) \leq 1 \ \forall v \in V$).

Fullständig matchning: Alla hörn ingår i M .

Maximal matchning: $|M|$ är maximalt.

För bipartita grafer säger vi att M är en fullständig matchning om:

$$|M| = |X| \leq |Y|, \quad G = (X \sqcup Y, E).$$

Halls sats (giftermålssatsen):

Om $G = (X \sqcup Y, E)$ är bipartit så har den en fullständig matchning omm:

$$|P(A)| \geq |A| \ \forall A \subseteq X$$

där $P(A) = \{y \in Y \mid \exists x \in A : xy \in E\}$.

En maximal matchning, M , av en bipartit graf har storlek $|M| = |X| - \delta(X)$, där $\delta(x)$ är G :s defekt:

$$\delta(G) = \max_{A \subseteq X} \{|A| - |P(A)|\} \geq 0$$

En matchning, M , i en bipartit graf, G , är maximal omm det inte finns en utökande alternerade stig för M i G .

Se nästsista övningsuppgiften i anteckningarna (uppgift 5, 2011-(05)maj-17) för en förklaring på utökande alternerande stigar.

Transversaler; att finna distinkta representanter. (Läs "DMF"-boken sida 244).

För en mängd mängder (en klass), välj en mängd med så få redan valda element som möjligt, och välj ett element (som inte redan valts i en annan mängd), det elementet är en distinkt representant för den mängden. Upprepa detta tilla alla mängder har en distinkt representant.

Mängden av representanterna är en transversal (den går genom alla mängderna).

Sammanfattningarnas

Sammanfattning

Modul 1

Division med rest
Konvertering av talbas
Delbarhet
Primtal
Största gemensamma delare
Delargrafer
Primtalsfaktorisering
Diofantiska ekvationer
Euklides' algoritm
Delbarhet av linjärkombination
Ekvationen $xm + yn = c$
Implikation av att ett primtal delar en produkt
Implikation av att ett primtal inte är en delare
 $d|mn, \text{sgd}(d; m) = 1 \Rightarrow ?$
Relativt prima tal
 $k|n, n|m \Rightarrow ?$
Minsta gemensamma multipel
 $\text{sgd}(m, n) \cdot \text{mgm}(m, n) = ?$
Kongruenta modulo m
Addition och multiplikation i \mathbb{Z}_n
Invertibla element i \mathbb{Z}_n och \mathbb{Z}_p
 $r \in \mathbb{Z}_m, \text{sgd}(r, m) = 1 \Rightarrow ?$
Ekvationen $ax = b$ i \mathbb{Z}_m
Mängdbyggare
 $\emptyset, \{\emptyset\}$ och \mathcal{U}
 $\mathbb{Z}, \mathbb{N}, \mathbb{Z}_+, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_m$
 $x \in A$ och $x \notin A$
 $A \subseteq B$ och $A \subset B$
 $A \cup B$ och $A \cap B$
 $A \setminus B$ och A^c
 $\mathcal{P}(A)$
 $C \subseteq A, A \subseteq B \Rightarrow ?$
Mängdlagar:
 Associativa lagen
 Kommutativa lagen
 Distributiva lagen
 De Morgans lag
 Identitetslagarna
 Absorptionslagen
 Dubbelt komplement
 Inverslagar
 Dominaslagar
 $|A \cup B|$

Kartetisk produkt: $A \times B$

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$$

Induktionsbevis

Rekursion

En funktions domän och kodomän

Sammansättning av funktioner

Injektion, surjektion och bijektion

Venn-diagram (för två mängder, vi har inte behandlar flertalet mängder)

Fibonaccitalen

Invers- och identitetsfunktioner

Kardinalitet

Uppräknerliga och överuppräknerna mängder

$$|\mathbb{Q}| = |\mathbb{N}| \because ?$$

$$|A|, |\mathcal{P}(A)|$$

Formell definition av relationer

Graf- och matrisrepresentation av en binär relation

Reflexiva, symmetriska, antisymmetriska samt transitiva relationer

Ekvivalensrelation

Ekvivalensklasser

Partialordning

Partitioner

Minimala, minsta, maximala och största element

Övre och undre begränsning

Modul 2

Additionsprincipen

Ramseytal

$|S|$, $r_x(S)$, $c_y(S)$

Multiplikationsprincipen

$P(A)$, A , ω , Ω

Likafördelning, $P(A) = \frac{|A|}{|\Omega|}$

Oberoende händelser

$P(A \cap B)$, $P(A \cup B)$

Ordnat/oordnat val med/utan upprepning

$(n)_m$, $n!$, $\binom{n}{k}$, $\binom{n}{k_1, \dots, k_n}$

$\binom{n}{k} = ? + ? = ?$

Pascals triangel

Binomialsatsen

Multinomialtal

Postfacksprincipen

Genererande funktioner

Sållprincipen

Stirlingtalen av andra slaget ($S(n, k)$)

Rekursionsformeln för $S(n, k)$

Antalet injektioner, surjektioner och bijektioner

Antalet ekvivalensrelationer

$P_k(n)$

Modul 3

Stela avbildningar

Definition av grupp

Grupptabeller

Abelska grupper

Latinska kvadrater hos grupper

$|G|$, $o(g)$

$|G| = ? \Rightarrow G$ abelsk

$o(g) = n \Rightarrow ?$

$o(g) = \infty \Leftrightarrow ?$

$o(g) = m, g^s = 1 \Leftrightarrow ?$

Delgrupper

$Z(G)$; G :s centrum och $C(G)$

$\langle g \rangle$

Sidoklasser

Lagranges sats

H :s index i G

Gruppisomorfi och grupphomomorfi

$U(G)$

Permutationer och dess:

Enradsnotation

Tvåradsnotation

Cykelnotation (med/utan reduktion)

Cykelstruktur

Produkt av cykelnotation

Permutationsmatris

$G \cong H \subseteq S_G$

π :s ordning utifrån π :s cykelstruktur

$\alpha, \beta \in S_n$ konjugerande omm ?

Transpositioner

Jämna och udda permutationer och antalet av dem

Paritet

$\text{sgn } \pi^{-1}$

$\text{sgn } \sigma \alpha \sigma^{-1}$

$\text{sgn } (x_1 \dots x_n)$

$\sum_{\pi \in S_n} \text{sgn } \pi \prod_{i=1}^n a_{\pi(i)i} = ?$

Ringar och kroppar (en. fields)

Normal grupp

Kvotgrupp

$\mathbb{R}[x]$

Modul 4

Felrättande kod $\mathcal{C} \subseteq \mathbb{Z}_2^n$, vad är n ?

\mathcal{C} :s viktiga egenskaper, och hur stora är de?

δ och $d(a, b)$ för \mathcal{C}

Sfärpackningssatsen och Hammingkoder, vad är en Hammingkod?

\mathcal{C} linjär omm ?

\mathcal{C} :s dimension

ω och ω_{\min} för en linjär kod

Paritetskontrollmatris och \mathcal{C} utifrån en sådan

\mathcal{C} rättar säkert ett fel om ?; hur hittar man fel i en sådan kod?

Kodord

(Asymmetriska) krypton

Fermats lilla sats, och en följsats med $m = (p - 1)(q - 1)$

RSA

Elektronisk signatur

Primtalens täthet

Fermattest

Psuedoprimtal

Carmichaeltal

Miller-Rabins test

Konnektiv: $\neg \wedge \vee \rightarrow \leftrightarrow \perp \top$, och ett till skrivsätt (för alla utom 2)

Kontraposition

Omvändning

Lagar inom boolesk algebra:

Kommutativitet

Associativitet

Distributivitet

De Morgan

Idempotens

Absorption

Involution

Komplementaritet

$\leftrightarrow, \rightarrow$ respektive \neg uttryckt

Boolesk algebra jämfört med mängdlära

Sanningsvärdestabeller för booleska funktioner och tolkning

Dualitet

Disjunktiv/konjunktiv (normal)form

Logiska kretsar

Karnaugh-diagram

Modul 5

Grannar
Varianter av grafer
 K_n , $K_{n,m}$, C_n
Grannlista
Grannmatris
Incidentmatris
Grafisomorfi
Valens
Udda hörn
Reguljaritet
Valenssumma
Vandring, väg, krets, stig, cykel
Sammanhängande grafer
Komponenter
Eulervägar/-kretser och Hamiltonstigar/-cykler
Träd, skog
Spännande träd, Kurskals algoritim
Binära rotade träd
Planära grafer, plana grafer
Ytor
Eulers polyederformel och generalisering
Krav för planaritet
Komplementgrafer, dualgrafer
Subdivision
Minor
Platonska kroppar
 $c(v)$, $\chi(G)$, $P_G(\lambda)$
Girig algoritim för ungefärligt värde på $\chi(G)$
6-, 5- och 4-färgssatserna
 $G - e$
 G/e
Rekursiv algoritim för $P_G(\lambda)$
Fullständiga och maximala matchningar
Halls sats (giftermålssatsen)
 $|M| = |X| - \delta(G)$
Utökande alternerande stig
Transversaler och distinkta representanter
Kuratowskis sats och Wagners sats