

# Lösningar till tentamensskrivning på kursen Algebra och kombinatorik för F3 maj 2002

1. Op. 1: Välj  $k$  lådor som skall vara tomma:  $\binom{n}{k}$  olika sätt.  
 Op. 2: Fördela  $r$  olika bollar i  $n - k$  icke-tomma delmängder:  $S(r, n - k)$  olika sätt.  
 Op. 3: Etikertera delmängderna:  $(n - k)!$  olika sätt.

Multiplikationsprincipen ger nu **SVAR.**  $\binom{n}{k} S(r, n - k) (n - k)!$ .

2. Låt  $x$  och  $y$  vara godtyckliga noder i grafen  $G$ . I  $G$  finns  $n - 2$  noder förutom noderna  $x$  och  $y$ . Till dessa  $n - 2$  noder går  $n - 1$  kanter från  $x$  och  $y$ . Alltså finns en nod  $z$  som träffas av minst två kanter från  $x$  och  $y$ . Eftersom  $G$  saknar multipla kanter måste en kant komma från  $x$  och en från  $y$ . Mellan  $x$  och  $y$  finns då en stig (av längd 2) och grafen är sammanhängande.

3. a) Subtraktion av ekvationerna ger  $x + 2y = 0$  och insättning i första ekvationen ger då  $y = 0$  och därmed  $x = 0$ . Alla dessa räkningar är utförda i  $Z_n$ , där  $n$  är godtyckligt.

b) Som ovan fast man får  $3y = 0$ . Två fall.

**Fall 1:** 3 delar inte talet  $n$ . Då är 3 inverterbart i  $Z_n$  och det finns bara den triviala lösningen  $x = 0, y = 0$ .

**Fall 2:**  $n = 3k$  för något heltal  $k$ . Ekvationen  $3y = 0$  har då lösningarna  $y = sk$  för  $s = 0, 1, 2$ . För var och en av dessa lösningar finns ett unikt tal  $x$  så att  $x + 2y = 0$ .

**Svar:** a) En lösning. b) En lösning om 3 inte delar  $n$ , om 3 delar  $n$  precis tre olika lösningar.

4. Vi betraktar det allmännare fallet med följder av längd  $n$ . Kalla en följd tillåten om ingen etta finns någonstans till höger om en tvåa. Låt  $a_n$  beteckna antalet tillåtna följder av längd  $n$ .

Vi listar upp alla tillåtna följder av längd  $n$ . Första listan innehåller de som börjar med en nolla. Efter nollan kommer en tillåten följd av längd  $n - 1$ . Denna lista innehåller alltså  $a_{n-1}$  stycken följder. Den andra listan som innehåller följder som börjar med en etta innehåller också  $a_{n-1}$  stycken olika följder. Den tredje listan innehåller följder som börjar med en tvåa. Efter denna två kommer antingen nollor eller tvåor, med inga restriktioner. Alltså innehåller denna lista  $2^{n-1}$  olika följder. Nu är alla följder upplistade och vi får då att

$$a_n = 2a_{n-1} + 2^{n-1}.$$

Motsvarande homogena rekursionsekvation har allmänna lösningen

$$a_n^h = C2^n$$

där  $C$  är en konstant. Vi ansätter kandidater till partikulärlösningar genom  $a_n^p = An2^n$  och får då att

$$An2^n = 2A(n-1)2^{n-1} + 2^{n-1}.$$

Denna ekvation ger att enda möjligheten för  $A$  är  $A = 1/2$ . Allmän lösning är alltså

$$a_n = C2^n + n2^{n-1}.$$

För  $n = 1$  gäller att  $a_1 = 3$  vilket ger att  $C = 1$ .

**Svar:**  $a_{20} = 2^{20} + 20 \cdot 2^{19}$ .

5. Låt  $a$  vara godtyckligt element i  $G$  och betrakta produkten av sidoklasserna  $aH$  och  $a^{-1}H$ . Denna produkt är en sidoklass  $cH$ . Denna sidoklass måste innehålla elementet  $a1a^{-1}1 = 1$ . Enda möjligheten är att  $cH = H$ . Elementen i mängden  $\{aha^{-1}1 \mid h \in H\} = aHa^{-1}$  är då en delmängd

till  $H$ . Då  $a$  var godtyckligt valt är  $H$  en normal delgrupp till  $G$ .

6. a) Kortast är kanske att konstatera att  $(z+1)(z^2+z+1) = 0$  dvs  $z^3+1 = 0$ . Men multiplikativa gruppen i  $K$  bestående av element skilda från noll består av sju element och inget av dessa har ordning tre och därmed är  $z^3+1 \neq 0$  för alla  $z \in K \setminus \{0\}$ . Inga rötter till andragradsekvationen  $z^2+z+1 = 0$  i  $K$  garanterar irreducibilitet då polynomets grad är just två.

b) Enligt lösningen ovan gäller att elementet  $z$  i en kroppsutvidgning av  $K$  med hjälp av polynomet  $z^2+z+1$  har ordningen tre. Om polynomet vore primitivt skulle  $z$  ha ordning  $8^2-1 = 63$ .

c) Trial and error ger oss polynomet  $z^2+z+x+1$ . Vi får att  $z^3 = xz+x+1$ ,  $z^6 = (z^3)^2 = x^2z+x$ ,  $z^7 = z \cdot z^6 = (x^2+x)z+x^2+x+1$ ,  $z^9 = z^2 \cdot z^7 = x+1$  och  $z^{21} = (z^9)^2 \cdot z^3 = z+x^2$ . Enda möjligheten för elementet  $z$  är då att det har ordning 63 eftersom dess ordning måste vara en delare till talet 63.

7. Representera problemet som en bipartit graf med nodmängderna  $P$  och  $F$ , pojkar respektive flickor, där vi har en kant mellan pojken  $p_i$  och flickan  $f_j$  om pojken  $p_i$  kan tänka sig bjuda upp flickan  $f_j$ .

Låt  $I$  beteckna en delmängd av pojkarna och  $J(I)$  de flickor som pojkarna i  $I$  kan tänka sig bjuda upp. Betrakta den delgraf som erhålles när bara noderna i  $I$  och  $J(I)$  finns kvar och kanter enligt ovan. Antalet kanter är då  $m|I|$  eftersom varje pojke i  $I$  kan tänka sig bjuda upp  $m$  stycken flickor. Några flickor i  $J(I)$  kan tänkas bli uppbjudna av andra pojkar än de i  $I$ , så från några noder i  $J(I)$  går eventuellt färre än  $m$  kanter till noderna i  $I$ . Vi kan därav sluta att  $|J(I)| \geq |I|$ . Enligt Halls sats finns, emedan  $I$  var godtycklig delmängd till  $P$ , en komplett matchning. Denna matchning låter vi utgöra första dansen.

Inför andra dansen gäller nu samma förutsättningar som från början men med  $m-1$  istället för  $m$ . Vi tillämpar nu Halls sats en andra gång och därefter en tredje gång osv.

8. a) Antalet ord i en perfekt binär ettfelsrättande kod  $C$  av längd  $n$  är enligt packningsvillkoret

$$|C| = \frac{2^n}{n+1}.$$

Antalet kodord i koden i konstruktionen ovan är

$$2^n \cdot |C| = 2^n \cdot \frac{2^n}{n+1} = \frac{2^{2n}}{n+1} = \frac{2^{2n+1}}{(2n+1)+1}.$$

Vi kontrollerar nu att minavståndet är tre.

Betrakta två kodord

$$(x_1 + c_1, x_2 + c_2, \dots, x_n + c_n, x_1, x_2, \dots, x_n, \sigma(x_1, x_2, \dots, x_n) + f(c_1, c_2, \dots, c_n))$$

och

$$(x'_1 + c'_1, x'_2 + c'_2, \dots, x'_n + c'_n, x'_1, x'_2, \dots, x'_n, \sigma(x'_1, x'_2, \dots, x'_n) + f(c'_1, c'_2, \dots, c'_n)).$$

Om  $\mathbf{x} = (x_1, \dots, x_n) = \mathbf{x}' = (x'_1, \dots, x'_n)$  så blir avståndet minst tre eftersom avståndet mellan  $\mathbf{c} = (c_1, \dots, c_n)$  och  $\mathbf{c}' = (c'_1, \dots, c'_n)$  är minst tre. Genom att betrakta fallen då avstånden mellan  $\mathbf{x}$  och  $\mathbf{x}'$  är ett, två och större än eller lika med tre får man på samma sätt att avstånden mellan kodorden är minst tre.

Då kodens minavstånd är tre så kommer sfärer med radien ett runt kodorden att vara disjunkta. Varje sådan sfär innehåller  $2n+2$  stycken ord. Enligt ovan innehåller koden  $\frac{2^{2n+1}}{(2n+1)+1}$  stycken ord. Totalt ligger alltså  $2^{2n+1}$  stycken ord på ett avstånd högst ett från ett kodord, dvs varje ord i  $Z_2^{2n+1}$  ligger på avståndet ett från ett kodord. Koden är därmed visad vara perfekt ettfelsrättande.

b) Vi låter  $f((0, 0, \dots, 0)) = 0$  och  $f((c_1, \dots, c_n)) \neq 0$  om  $(c_1, \dots, c_n) \neq (0, \dots, 0)$ . Summan av två ord i koden som inte är nollordet ligger då aldrig i koden. Koden är då inte linjär.