Diskret matematik - repetition

Funktion

En funktion $f : A \to B$ är en regel som för varje element a i A ordnas till precis **ett** element b i B.

En funktion är **injektiv** om $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$. Ett element i B får träffast högst en gång.

En funktion är **surjektiv** om $\forall b \in B, \exists a \in A$ så att $f(a) = b$. Alla element i B träffas minst en gång.

En funktion är **bijektiv** om den är både injektiv och surjektiv. En sådan funktion är inverterbar.

Antalet funktioner från mängden X till mängden Y är $|Y|^{|X|}$ då varje element i X har Y element att välja mellan.

Bijektioner mellan två mängder finns enbart för mängder av samma storlek (eller oändliga).

Kardinalitet

Två mängder har samma kardinalitet om det finns en bijektiv funktion (bijektion) mellan dem. En sådan mängd är uppräknelig. Med en oändlig, uppräknelig mängd kan ett ändligt antal element tas bort utan att påverka kardinaliteten.

Ring

En mängd och två räknesätt är en kropp $(K, +, *)$ om $(K, +)$ är en grupp och $(K, *)$ är en grupp. Enbart additionen måste vara kommutativ, $a * b = b * a$ och $a + b = b + a$. Multiplikationen behöver inte ha en invers för 0. Exempelvis de hela talen, $\mathbb{Z}$.

Kropp

En mängd och två räknesätt är en kropp $(K, +, *)$ om $(K, +)$ är en grupp och $(K \setminus \{0\}, *)$ är en grupp. Multiplikationen och additionen måste vara kommutativ, $a * b = b * a$ och $a + b = b + a$. Exempelvis $\mathbb{R}$ (oändlig).

Viktig sats:

Om p är ett primtal är $(\mathbb{Z}_p, +, *)$ en kropp.

Rekursionsekvation

Om det enbart finns ett värde för r (dubblerot / trippelrot o.s.v.) så sätts $r_n = (K_1 + K_2 n)r^n$ eller $r_n = (K_1 + K_2 n + K_3 n^2)r^n$ o.s.v.

Visualisera med hjälp av matriser

1. Ordna elementen i A (numrera 1 till n)
2. Bilda en $n \times n$-matris likt följande

$$M = (m_{ij}) \text{ där } m_{ij} = \begin{cases} 1 & \text{om } {}_iR_j \\ 0 & \text{om } {}_iR_j \end{cases}$$

En sammansatt funktion på matrisform beräknas med vanlig matrismultiplikation, där allt över 0 blir 1. D.v.s $R_1 \circ R_2 = M_1 \times M_2$.

I en matris ser man att en relation är :

- **reflexiv** genom att kontrollera att huvuddiagonalen enbart består av ettor
- **symmetrisk** genom att kontrollera att det finns en symmetri, d.v.s att element $(i, j) = (j, i)$
- **transitiv** genom att kontrollera att $M \times M = M$
- **anti-symmetrisk** genom att kontrollera att det inte finns någon symmetri. D.v.s. att om elementet $(i, j) = 1$ så är garanterat $(j, i) = 0$, vice versa.

Sammansatta relationer

Den sammansatta relationen av två relationer R_1 och R_2 betecknas $R_1 \circ R_2$ och definieras enligt

$$(a, c) \in R_1 \circ R_2 \text{ om det finns något } b \in A \text{ sådant att } (a, b) \in R_1 och (b, c) \in R_2$$

Ekvivalensrelationer

En ekvivalensrelation är en relation som är **reflexiv**, **symmetrisk** och **transitiv**. Exempelvis $=, \equiv$ och "har samma länd som".

Ekvivalensklasser

Givet en ekvivalensrelation R på en mängd A kan man definiera ekvivalensklasser som

$$E_x = \{y \in A|_x R_y\}$$

E_x kallas för **ekvivalensklassen för** x och består av alla element i A som är ekvivalenta med x .

Notera att man ofta skriver $E_{\overline{x}}$. "Elementet" $\overline{x}$ sägs vara represent för E_x (eller $E_{\overline{x}}$).

Partiella ordningsrelationer

En partiell ordningsrelation är en relation som är **reflexiv**, **anti-symmetrisk** och **transitiv**. Exempelvis $\leq, \subseteq$ och "chef över".

Totala ordningsrelationer

En total ordningsrelation är en partiell ordningsrelation sådan att för alla $x, y \in A$ gäller ${}_xR_y$ eller ${}_yR_x$.

Partitioner

Låt M vara en mängd. En samling av (ändligt eller oändligt) många icke-tomma delmängder av M, $x_1, x_2, \ldots$ kallas för partitioner av M om följande uppfylls

- Får ej överlappa, $x_i \cap x_j = \emptyset$ om $i \neq j$
- Alla partitioner blir mängden själv, $x_1 \cup x_2 \cup \ldots = M$

Notera att varje ekvivalensrelation ger upphov till en partition.

Antalet ekvivalensrelationer på en mängd är alltså antalet partitioner av mängden.

Grupper

En grupp $(G, *)$ består av en icke-tom mängd G och en binär partition $* : G \times G \to G$.

Notera att '$*$' här innebär "grupp-multiplikation".

En grupp har följande egenskaper:

1. Den är sluten. $\forall x, y \in G$ gäller $x * y \in G$
2. Den är associativ. $\forall x, y, z \in G$ gäller $(x * y) * z = x * (y * z)$
3. Den har ett identitetselement. $\exists e \in G$ så att $x * e = e * x = x, \forall x \in G$. Kallas även det neutrala elementet e. **Detta element är unikt**
4. Det ska finnas inverser. $\forall x \in G$ finns något $y \in G$ så att $x * y = y * x = e$. Elementet y betecknas med x^{-1} och kallas för inversen till x

Notera att grupper som har egenskapen $x * y = y * x, \forall x, y \in G$ sägs vara abelska (kommutativa).

Symmetriska grupper

En symmetrisk grupp betecknas S_n eller σ_n där n är antalet element som ordnas i tuplar, triplar etc. S_n har $n!$ element (antalet sätt n element kan ordnas).

Ordningen för en grupp

Låt $(G, *)$ vara en grupp. Då definieras ordningen av gruppen som $|G|$.

Det vill säga att ordningen för en grupp definieras som antalet element i gruppen.

Ordningen för ett element i en grupp

Låt $g \in (G, *)$. Då definieras ordningen av elementet i gruppen som

$$ord(g) = \begin{cases} min\{m \in \mathbb{Z}_+ | g^m = e\} \\ \infty, \ g^m \neq e, \forall m \in \mathbb{Z}_+ \end{cases}$$

Det vill säga att ordningen för ett element är det minsta heltalsvärdet för $m \geq 1$ så att g^m är lika med identitetselementet. Om det inte finns något sådant värde för m definieras ordningen som ∞.

Delgrupper

Låt $(G, *)$ vara en grupp. Låt H vara en delmängd till G så att:

1. Sluten
2. Identitetselementet är medtaget
3. Alla inverser är medtagna

då är $(H, *)$ en **delgrupp** till $(G, *)$.

Gruppen $< g >$

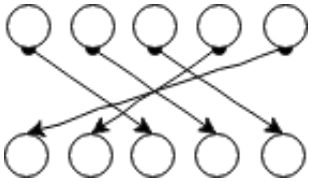
Gruppen $< g >$ kallas för **gruppen som genereras av** g. Grupper som genereras av **ett** element sägs vara cykliska.

Exempelvis är gruppen $(\mathbb{Z}, +)$ en grupp som genereras av 1 (eller -1) och är cyklisk.

Symmetriska grupper (permutationer)

Betrakta den symmetriska gruppen $(S_5, \circ)$.

Då är σ_{34521} en permutation,



För att få fram en cykelform för enradsform skrives först denna om som tvåradsform genom att låta den övre raden vara de ordnade värdena. Sedan följs samma resonemang som nedan.

För att få fram en cykelform för tvårads skrives först enradsformen om till tvåradsform där den övre raden består av ordnade tal. Sedan följes cykeln, från övre raden, värde 1 till värdet under 1, här 3. Sedan går man från övre raden, här värde 3 och följer den nedåt.

För att invertera en cykelform läses ingående element baklänges, här $(5\ 3\ 1)(4\ 2)$.

För att invertera en tvåradsform skiftas de bägge raderna.

För att invertera en enradsform skrivs denna först i tvåradsform med ordnade ovanstående element. Sedan skiftas de bägge raderna.

Typen av en permutation

Typen av en permutation beskriver längderna för dess ingående cykler. Det vill säga, cykeln $\underbrace{(1\ 3\ 5)}_{3}\underbrace{(2\ 4)}_{2}$ är av typ $\{3, 2\}$.

Ordningen av en permutation

Ordningen av en permutation är alltid lika med LCM av cykellängderna. Detta då cykelna måste vara i fas för att ge identitetselementet. I ovanstående fall är $LCM(3, 2) =$ och därmed är permutationen av ordning 6.

Transposition

En transposition är en permutation som byter plats på två element. Varje permutation kan skrivas som en produkt (sammansättning) av transpositioner.

För att faktorisera σ till produkter av transpositioner utgår man från permutationen och byter plats på två element i taget till dess att den ordnade permutationen ($\sigma_{12345\ldots}$). Faktoriseringen är sedan sammansättningen av samtliga transpositioner, uppifrån ned.

Om en permutation kan skrivas som en produkt av ett **jämnt** antal transpositioner kallas denna **jämn**. Annars är permutationen **udda**. Notera att detta är oavsett hur transpositionen görs, det vill säga att den **alltid** utförs på ett jämnt antal **eller** udda antal transpositioner.

RSA

Att skapa nycklar

1. Välj två olika (slumpmässiga) primtal p och q
2. Beräkna $n = pq$
3. Beräkna $m = (p-1)(q-1)$
4. Bestäm två tal e och d så att $e * d \equiv 1 \ (mod \ )$m

Notera att vi kan välja $1 < e < m$ så att $GCD(e, m) = 1$ (relativt prima). $ed = 1 + km$ har en entydig lösning. Hittas med Euklides algoritm.

Steg 2 samt värdet e är offentliga. Steg 3 samt värdet d är hemliga. e är den publika nyckeln (*encrypt*). d är den privata nyckeln ($decrypt$).

Kryptering

Omforma meddelandet a till $0 \leq a \leq n$. Använd sedan den offentliga nyckeln och beräkna det krypterade meddelandet $y \equiv a^e \ (mod \ n)$. y väljs så att $0 \leq y \leq n-1$.

Dekryptering

Vi har mottagit y och vill veta a. Vi använder den hemliga nyckeln och beräknar $a' \equiv y^d \ (mod \ n)$ och väljer a' så att $0 \leq a' \leq n-1$.

Olika typer av grafer

En **multigraf** får ha flera kanter mellan samma par av noder.

En **riktad graf** har kanter med riktningar. Ordningen på u och v spelar roll, "från, till".

Graden för en nod är antalet kanter som går till noden.

En **fullständig** / **komplett** graf har med alla kanter. Tecknas k_n. En komplett graf har $\frac{n(n-1)}{2}$ kanter. Antalet grafer med n noder är därav $2^{n(n-1)/2}$. Ingen komplett graf förutom k_1 och k_2 är bipartit.

En **vandring** är en följd av noder $v_1, v_2, \ldots, v_n$ där $\{v_i, v_{i+1}\} \in E, i = 1, \ldots, k-1$.

En **väg** är en vandring där alla kanter är olika. Det vill säga ej upprepning hos kant.

En **stig** är en vandring där alla noder är olika.

En **krets** är en snluten väg där startnod och slutnod är samma, $v_1 = v_k$.

En **cykel** är en sluten stig. Här får startnoden besökas två gånger.

En **Eulersk väg/krets** besöker alla kanter. Man kan bestämma om en sådan finns genom att kontrollera att den är sammanhängande och att alla noder har jämn grad, utom 2 (start/stop) eller 0 (de med udda).

En **Hamiltonsk stig/cykel** besöker alla noder. Det finns inget lätt sätt att se om en graf är Hamiltonsk. Däremot vet man att den definitivt inte är det om det finns minst 3 noder med grad 1.

En **isomorfisk graf** är på samma form - om de har samma duala graf.

Komplementgrafen $\overline{G}$ till G har $\overline{E} = v^2 - E, v^2 = \{\{u, v\} | u, v \in V, u \neq v\}$.

Vissa grafer tillåter att nodmängden V kan delas upp i V_1 och V_2 så att $\{u, v\} \notin E$ om $u \in V_1$ och $v \in V_2$. Detta är en **bipartit graf**. Kan tolkas som "inga kanter mellan noder på samma mängd".

En **stjärngraf**, s_n har en nod i mitten som samtliga andra noder är kopplade till. Övriga noder kopplas ej till varandra. En stjärngraf är alltid bipartita.

En **kubgraf**, c_n ser ut som en 3D-kub.

Den **fullständiga bipartita grafen** $k_{n,m}$ har $n + m$ noder, $|v_1| = n, |v_2] = m$ och **alla** möjliga kanter, $|E_{n,m}| = nm$.

Ett **träd**. Inga cykler.

Eulers formel

I varje sammanhängande graf $G = (V, E)$ gäller att $v - e + f = 2$ där $v = |V|, e = |E|$ och f antalet fasetter.

Ordnade urval

	Utan hänsyn till ordningen	Med hänsyn till ordningen
Utan återläggning	$\binom{n}{r}$	$P(n, r) = \frac{n!}{(n-r)!}$
Med återläggning	$\binom{n+r-1}{r}$	n^r

Utan hänsyn till ordningen, med återläggning:

En pappa ska fördela 12 kinderägg bland sina 4 barn. På hur många sätt kan detta ske?

Man tänker att man har 12 kinderägg och $4 - 1$ seperatorer som delar upp mängden i delar. Vi behöver då $12 + 4 - 1 = 15$ platser och vi väljer ut 12. Alltså $\binom{4+12-1}{12}$.