IMAx2022-LF-Kont-Aug2022

Hans Jakob Rivertz

September 2022

Oppgave 1 og 2. Arganddiagram

Oppgaven gikk ut på å finne og representere mengden av alle punkt z som oppfyller likningen $|z-(1+i)|=1$ i et Argand diagram.
Løsning: Erstatt z men dens kartesisk form $z = x + iy$.

$$|x+iy-(1+i)| = 1.$$

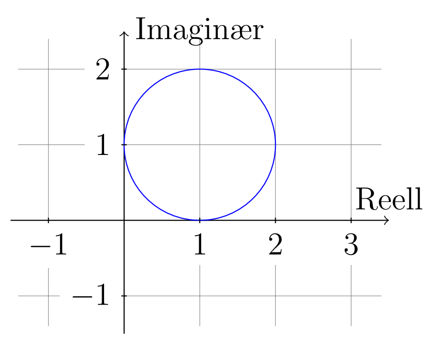
Samle realdel og imaginærdel for seg.

$$|(x-1)+i(y-1)| = 1.$$

Bruk formel for absoluttverdi av komplekst tall: $|x+iy| = \sqrt{x^2+y^2}$

$$\sqrt{(x-1)^2+(y-1)^2} = 1.$$

Dette er likningen for en sirkel med radius 1 og senter i punktet $(1, 1)$.



Oppgave 3, egenverdier

Oppgaven var å svare på hvilke av tre oppgitte vektorer er egenvektorer til matrisen og finne egenverdien i tilfelle vektoren er en egenvektor.

$$A = \begin{bmatrix} 1 & 3 & 6 \\ 2 & 1 & 4 \\ 1 & 0 & 3 \end{bmatrix}$$

a) $v_1 = [1, 3, -2]^T$. Regner ut $Av_1 = [-2, 3, -5]^T$, som ikke er en egenvektor da $1\lambda = -2$, $3\lambda = 3$, $-2\lambda = -5$ ikke har noen løsning.

b) $v_2 = [-2, -2, 1]^T$. Regner ut $Av_2 = [-2, -2, 1]^T$, som er en egenvektor med egenverdi 1.

c) $v_3 = [0, 1, -5]^T$. Regner ut $Av_3 = [-27, -19, -15]^T$, som ikke er en egenvektor da $0\lambda = -27$ ikke har noen løsning.

Oppgave 4, Kryptografi

a) Løs for x i den lineære kongruensen $3x \equiv 1 \pmod{40}$, ved bruk av Euklids utvidete algoritme.

Løsning: Deler 40 med 3 og får 13 med 1 i rest. Det betyr at $1 = 40 - 3 \cdot 13$. Derfor er $1 \equiv 3 \cdot (-13)$. Et svar er derfor -13. Et annet godkjent svar er $-13 + 40 = 27$.

Pers offentlige RSA krypteringsnøkkel er gitt ved n=55 og e=3.

b) Finn Pers hemmelige nøkkel, dvs. finn primtallene p og q, og eksponenten d.

Løsning: Primtalls-faktoriseringen til $n = 55$ er $55 = 11 \cdot 5$. La $p = 5$ og $q = 11$. Den hemmelige nøkkelen er det minste positive tallet d som er invers til $e = 3$ modulo $(p-1)(q-1) = 40$. Oppgave a) ga oss svaret 27.

En strengere form for RSA bruker $\text{lcm}(p-1, q-1) = 20$ istedet for $(p-1)(q-1) = 40$. Du ville da fått svaret $d = 7$.

c) Hvilke av følgende verdier for e kunne Per også brukt, med samme n=55? Vi tenker ikke på hvor sikkert et slikt valg ville være, men på verdier for e som er gyldige.

Løsning: Poenget er at e og 40 må være relativt primiske (også kalt innbyrdes primiske). I listen {2,4,5,6,7,9} er det kun 7 og 9 som kan brukes.

Du ville fått samme svar om du brukte 20 istedet for 40.

d) Krypter meldingen $M = 15$ med nøkkelen gitt i punkt a).

Løsning: Du bruker nøkkelen $e = 3$ og regner ut $15^3 \pmod{40}$. Det kan gjøres på mange måter. For eksempel kan vi gjøre det i to trinn $15^2 = 225 \equiv 5 \pmod{40}$, fordi $5 = 225 - 4 \cdot 55$. Deretter regnes $15^3 = 15^2 \cdot 15 \equiv 5 \cdot 15 = 75 \equiv 20 \pmod{40}$.

Vi kunne også regnet ut $15^3 = 3375$, dividert på 55 og funnet resten 20.

Oppgave 5, Funksjoner AtB

La $A = \{0, 1, 2, 3\}$, $B = \{3, 4, 5, 6, 7, 8\}$.

i) Hvor mange forskjellige funksjoner $f : A \to B$ er det?

Løsning: For hvert av de fire elementene i A kan bildet velges fritt fra de 6 elementene i B. Det gir $6^4 = 1296$ forskjellige funksjoner.

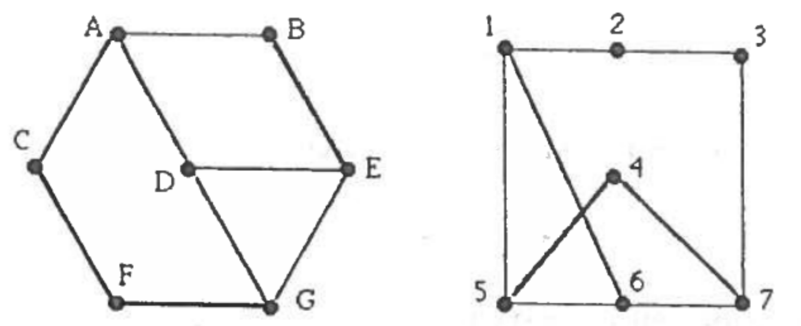
ii) Hvor mange av funksjonene i i) er injektive (en-til-en)?

Løsning: Dette er det samme som ordnet utvalg uten tilbakelegging. Svaret er derfor $6P4 = \frac{6!}{2!} = 360$.

Alternativ løsning: Det er 6 mulige valg for bildet av 0. Deretter er det 5 mulige valg for bildet av 1, 4 mulige valg for bildet av 2 og til slutt 3 mulige valg for bildet av 3. Vi bruker produktregel og får $6 \cdot 5 \cdot 4 \cdot 3 = 360$.

Oppgave 6, Isomorfi

Definer eksplisitt (f.eks.. ved en tabell eller liste) en funksjon $f : \{A, B, C, D, E, F, G\} \to \{1, 2, 3, 4, 5, 6, 7\}$ mellom nodene til de to grafene i figuren som gir en isomorfi mellom grafene.



Løsning En isomorfi er en kantbevarende bijektiv avbilding mellom nodene.

(1) En isomorfi bevarer kretser. Det er en krets av lengde 3 i hver figur. Derfor må $\{D, E, G\}$ sendes til $\{1, 5, 6\}$.

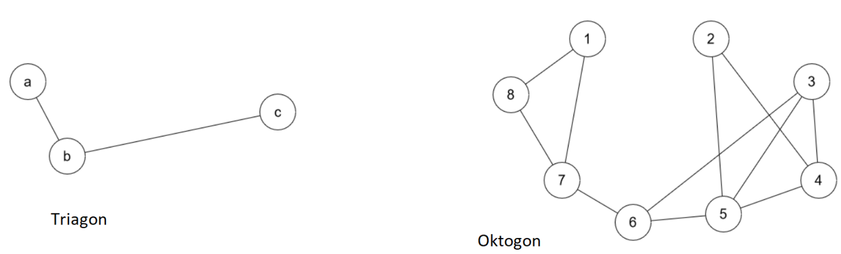
(2) Den må bevare gradene til punktene. Det er fire punkter av grad 3. Derfor må $\{A, D, E, G\}$ sendes til $\{1, 5, 6, 7\}$. Tre av disse er i kretsene fra (1). Derfor må $f(A) = 7$.

(3) Det er en krets med lengde 5 i hver av figurene $A - C - F - G - D$ og $7 - 3 - 2 - 1 - 6$. Disse har grader $3, 2, 2, 3, 3$. Defor er $f(C) = 3$, $f(F) = 2$, $f(G) = 1$ og $f(D) = 6$.

(4) Det er to punkter igjen i hver graf $\{B, E\}$ og $\{4, 5\}$. Fra gradene ser vi at vi må ha $f(B) = 4$ og $f(E) = 5$.

(5) Det gjenstår å sjekke om kanter avbildes på kanter.

Oppgave 7, Olav og Eirik



Olav den Uheldige har bygga seg ei lita festning Triagon og ei stor festning Oktogon for å forsvare seg fra naboen, Eirik den Stygge. Triagon hadde 3 tårn, Oktogon hadde 8 tårn, og Olav har gravd en brønn i hvert av 11 tårn. Hvert par av brønner i samme festning hadde ei vannledning som kobla dem sammen. Det var ikke vannledninger mellom festninger.

I løpet av noen år klarte Eirik sine menn å ødelegge noen vannledninger, slik at resterende vannledninger i henholdsvis Triagon og Oktogon kan representeres på følgende kart.

A. Hvor mange vannledninger i Triagon har Eirik&Co ødelagt? Begrunn svaret.

Løsning: Vi bruker at nettverket av rør er en komplett graf med 3 noder. Den komplette grafen med k hjørner har $\binom{k}{2}$ kanter. For $k = 3$ er det $\binom{3}{2} = 3$ kanter. Det er igjen 2 kanter derfor er det fjernet $3 - 2 = 1$ kant.

B. Hvor mange vannledninger i Oktogon har Eirik&Co ødelagt? Begrunn svaret.

Løsning: Begrunnelsen er som i oppgave A. For $k = 8$ er det $\binom{8}{2} = 28$ kanter. Det er igjen 11 kanter derfor er det fjernet $28 - 11 = 17$ kanter.

Eirik ønsker å forgifte forsvarerne av begge festningene, og har fått tak i gift. Dersom giften slippes i en brønn, så sprer den seg over alle vannledninger som går ut fra brønnen slik at alle nabobrønnene er forgifta om ett døgn. Og så sprer giften seg videre til andre brønner på samme måte.

Eirik vil spare sine egne menn. Derfor har han bestemt å velge bare ett tårn i hver festning som kommer til å bli forgifta. Deretter vil giften spre seg selv, og Eirik ønsker at alle brønnene i hver festning blir forgifta fortest mulig.

Du er ansatt som giftteknisk ingeniør til Eirik den Stygge, og han ber deg om å velge riktig starttårn med utgangspunkt i kartet ovenfor.

C. Dersom Eirik sitt ønske skal bli oppfylt, hvilket tårn skal være forgiftet først i Triagon festning? Begrunn svaret.

Løsning: Han må forgifte brønn nummer b. Da tar det ett døgn før de to andre brønnene er forgiftet. De to andre krever to døgn da giften må innom brønn b for å spre seg til hele festningen.

D. Dersom Eirik sitt ønske skal bli oppfylt, hvilket tårn skal være forgiftet først i Oktogon festning? Begrunn svaret.

Løsning: Tårn 6 må forgiftes først. Da tar det et døgn til nabobrønnene 7, 3 og 5 er forgiftet. I løpet av det neste døgnet forgiftes brønn 1 og 8 fra brønn 7, brønn 2 forgiftes fra brønn 2 og brønn 4 forgiftes fra brønn 3 og 5. Da er hele brønnen forgiftet på to døgn. Løsningen 6 er den eneste løsningen. Om man starter i en annen node må man gjennom node 6 for å komme til den andre siden av grafen. Det vil derfor ta minst et døgn lenger.

Du er fortsatt Eirik sin giftteknisk ingeniør, men i tillegg er du en hemmelig agent av Olav den Uheldige. (Da vil du så klart at det finns ei brønn uten gift i hver festning så langt som mulig.)

E. Hvilket tårn i Triagon skal du anbefale til Eirik i så fall?

Løsning: Da må man forurense brønn a eller c. Da vil det ta to døgn innen de to andre nodene er forurenset.

F. Hvilket tårn i Oktogon skal du anbefale til Eirik i så fall?

Løsning: Fra node 8 og 1 vil det ta to døgn før node 6 er forurenset. Tilsvarende tar det to døgn fra node 2 og 4 er forurenset til 6 er forurenset. Deretter bruker vi oppgave D til å vise at det tar ytterligere to dager. Svaret er 4 dager.

G. Hvilke grafteoretiske begreper og algoritmer klarer du å se i problemstillinga om Olav og Eirik?

Løsning: Sammenhengende grafer, noder, kanter, komplette grafer, vi kunne nevne flere.

1 Oppgave 8, Analyse

Besvarelsen av denne oppgaven skal skrives i feltet nedenfor. Tips: Bruk notasjonen f_x, f_y, etc for å lette skrivingen din.

Gitt funksjonen $f(x,y) = x^2y + 4xy - y^3 + 6y^2 - 5y$.

a) Regn ut de partielle deriverte av første orden av funksjonen $f(x,y)$.

Løsning:

$$
\begin{aligned}
f_x(x,y) &= 2xy + 4y = 2y(x+2) \\
f_y(x,y) &= x^2 + 4x - 3y^2 + 12y - 5
\end{aligned}
$$

b) Regn ut de partielle deriverte av andre orden

Løsning:

$$
\begin{aligned}
f_{xx}(x,y) &= 2y \\
f_{yx}(x,y) &= 2x + 4 \\
f_{xy}(x,y) &= 2x + 4 \\
f_{yy}(x,y) &= -6y + 12
\end{aligned}
$$

c) Finn alle kritiske punkter til funksjonen $f(x,y)$. **Løsning:** Vi løser likningene $f_x(x,y) = f_y(x,y) = 0$: Den første likningen; $f_x(x,y) = 2y(x+2) = 0$ er tilfredsstilt når $y = 0$ eller $x = -2$. Vi setter $y = 0$ inn i den andre likningen; $f_y(x,0) = x^2 + 4x = 0$ som har løsning $x = 0$ eller $x = -4$. Vi setter $x = -2$ inn den andre likningen; $f_y(-2,y) = -3y^2 + 12y - 9 = 0$ som har løsning $y = 1$ eller $y = 3$. Vi oppsummerer: De kritiske punktene er $(0,0)$, $(-4,0)$, $(-2,1)$, og $(-2,3)$.

d) Klassifiser de kritiske punktene du fant i c).

Løsning:

(x,y)	$A = f_{xx}$	$B = f_{yy}$	$C = f_{xy}$	$D = AB - C^2$	Type
$(0,0)$	0	12	4	-16	sadel
$(-4,0)$	0	12	-4	-16	sadel
$(-2,1)$	2	6	0	12	min
$(-2,3)$	6	-6	0	-36	sadel

Oppgave 9, Logikk

Gitt følgjande to utsagn p = "Det er vinter", q = "Det er kaldt ute". Velg setningen som har samme eller ekvivalent logiske struktur som de sammennsatte utsagnene.

1. $\neg\, p$

   Løsning: Den første er riktig fordi den er sann når p ikke er sann.

   X Det er ikke vinter
   - Det er sommer
   - Det er vinter
   - Det er ikke kaldt inne
   - Det er kaldt inne

2. $p \to q$

   Løsning: Den første er riktig. Da denne betyr hvis p så q.

   X Hvis det er vinter så er det kaldt ute.
   - Det er vinter, derfor er det kaldt
   - Det er vinter og det er kaldt.
   - Det er kaldt og det er ikke vinter
   - Jeg fryser.

3. $\neg\, p \vee q$ **Løsning:** Bruk omskrivningsregelen $\neg\, p \vee q \equiv p \to q$. Svaret er det samme som i b).

   X Hvis det er vinter så er det kaldt ute.
   - Det er ikke vinter og er det kaldt ute.
   - Det er ikke kaldt ute eller det er ikke vinter.
   - Ingen av alternativene er riktige.
   - Hvorfor handler denne oppgaven om vinter og kulde når det fortsatt er sommer?

4. $\neg\, (p \wedge q)$

   Løsning: De Morgans regel gir $\neg\, (p \wedge q) \equiv \neg p \vee \neg q$ som er første alternativ.

   X Det er ikke vinter eller det er ikke kaldt ute.
   - Det er ikke vinter og det er ikke kaldt ute.
   - Det er vinter og det er kaldt ute.
   - Det er vinter eller det er kaldt ute.
   - Endelig en oppgave som passer med at det er august.

5. $\neg\, q \to \neg\, p$

   Løsning: $\neg\, q \to \neg\, p$ er den kontrapositive formen av $p \to q$ som er det samme som b)

   X Hvis det er vinter så er det kaldt ute.

- Hvis det ikke er kaldt ute så er det vinter.
- Det er ikke kaldt ute og det er ikke vinter.
- Ingen av alternativene er riktige.
- Dere burde ikke stille så vanskelige spørsmål.
- Hvis det er varmt ute så er det sommer.