

Datalogi intro Opgaver

Kristoffer Klokke

2021

Contents

36 Uge	17
36.1 Konvertér følgende tal i 2-talsystemet (binær repræsentation) til 10- talsystemet	17
36.2 Konvertér følgende tal i 3-talsystemet til 10-talsystemet	17
36.3 Konvertér følgende hexadecimale udtryk, set som tal i 16-talsystemet, til tal i 10-talsystemet	17
36.4 Konvertér følgende hexadecimale udtryk til bitstreng	17
36.5 Konvertér følgende bitstreng til hexadecimale udtryk	17
36.6 Lav følgende additioner i 2-talsystemet (binær repræsentation)	18
36.7 Konvertér følgende tal i 10-talsystemet til 2-talsystemet (binær repræsentation)	18
36.8 Konvertér følgende tal i 10-talsystemet til 3-talsystemet	18
36.9 Konvertér følgende tal i two's complement (8 bits) til 10-talsystemet	18
36.10Vend fortegnet på følgende tal i two's complement (8 bits) . .	18
36.11Konvertér følgende tal i 2-talsystemet med fast decimalpunkt til 10 talsystemet	19
36.12Konvertér følgende tal i 2-talsystemet fra fast decimalpunkt til flyden- de decimalpunkt (med notationen fra slides for 8 bits flydende decimalpunktstal)	19
37 Uge	19
37.1 Konvertér følgende tal i 2-talsystemet (binær repræsentation) til 10-talsystemet	19
37.2 Konvertér følgende tal i 3-talsystemet til 10-talsystemet	19
37.3 Konvertér følgende hexadecimale udtryk, set som tal i 16-talsystemet,til tal i 10-talsystemet	19
37.4 Konvertér følgende hexadecimale udtryk til bitstreng	20
37.5 Konvertér følgende bitstreng til hexadecimalt udtryk	20
37.6 Lav følgende additioner i 2-talsystemet (binær repræsentation)	20
37.7 Konvertér følgende tal i 10-talsystemet til 2-talsystemet (binær repræsentation)	20
37.8 Konvertér følgende tal i 10-talsystemet til 3-talsystemet	20
37.9 Konvertér følgende tal i two's complement (8 bits) til 10-talsysteme	20
37.10Vend fortegnet på følgende tal i two's complement (8 bits) . .	21
37.11Konvertér følgende tal i 10-talsystemet til 8 bits two's complement	21

37.12	På slides om repræsentation af tal er der angivet en metode til at skifte fortegn på heltal repræsenteret i two's complement. Her er en anden metode. Inverter alle bits i tallet og læg derefter 1 til tallet. Find et argument for, at de to metoder gør det samme. Forklar argumentet klartest muligt for hinanden	21
37.13	Konvertér følgende tal i 2-talsystemet med fast decimalpunkt til 10-talsystemet	21
37.14	Konvertér følgende tal i 2-talsystemet fra fast decimalpunkt til flydende decimalpunkt - 8 bits notation	21
37.15	Konvertér følgende tal i flydende decimalpunkt (med notationen fra slides for 8 bits flydende decimalpunktstal) til 2-talsystemet med fast decimalpunkt, og derefter til 10-talssystemet	22

38 Uge 22

38.1	Hvad er output af kredsløbet nedenfor?	22
38.2	Hvad er værdien af nedenstående Boolske udtryk hvis (x_1, x_2, x_3) er lig $(0, 1, 0)$? Opskriv et kredsløb svarende til udtrykket. $(x_1 \wedge x_2) \oplus (x_3 \vee (\neg x_1))$	22
38.3	Opskriv et Boolsk udtryk om svarer til nedenstående kredsløb. For hvilke værdier af x, y og z vil kredsløbet kredsløbet nedenfor give output 1? Opskriv hele tabellen for kredsløbet. . .	23
38.4	Lav et Boolsk udtryk med NOT, AND, OR og tre input variable, som har nedenstående tabel. Tegn også et tilsvarende kredsløb med tre inputs.	23
38.5	Vis hvordan man kan lave en OR-gate ved hjælp af AND-gates og NOT-gates. (Til forelæsningen blev det vist, at alle boolske funktioner kan implementeres med AND-, OR-, og NOT-gates. Opgaven her viser, at AND- og NOT-gates er nok.)	24
38.6	Vis hvordan man kan lave en NOT-gate ved hjælp af en NAND-gate. Vis derefter hvordan man kan lave en AND-gate ved hjælp af NAND-gates. (Sammen med opgaven ovenfor viser dette, at NAND-gates er nok til at implementere alle boolske funktioner.)	24
38.7	[Repetition fra forelæsningen.] Opskriv den korrekte tabel for funktionen Resultat(x_1, x_2, x_3) fra slides om gates.	25
38.8	Opskriv tabellen for nedenstående kredsløb. Hvilken enkeltgate svarer det til?	25
38.9	Hvad er output af kredsløbet nedenfor?	26
38.10	Opskriv et Boolsk udtryk som svarer til samme kredsløb. Opskriv hele tabellen for kredsløbet.	26

38.11	Lav et Boolsk udtryk med NOT, AND, OR og tre input variable, som har nedenstående tabel. Tegn også et tilsvarende kredsløb med tre inputs.	27
38.12	[Repetition fra forelæsningen.] Opskriv den korrekte tabel for funktionen $Mente(x_1, x_2, x_3)$ fra slides om gates.	27
38.13	Repetér hvordan I lærte i folkeskolen at gange flercifrede tal i 10-talsystemet sammen (på papir, uden lommeregner). Lav f.eks. regnestykkerne $123 \cdot 432$ og $321 \cdot 765$. Overvej hvorfor det virker (husk definitionen af 10-talsystemet, se evt. slides). Brug derefter samme princip til at lave en gangemethode i 2-talsystemet. Lav f.eks. regnestykkerne $111_2 \cdot 101_2$ og $10110_2 \cdot 11110_2$ på denne måde. Check at du har regnet rigtigt ved at konverterer de fire tal samt de to resultater fra 2-talsystemet til 10-talsystemet og derefter gange sammen på lommeregner der. Forklar metoden, og argumentet for at den fungerer, klarest muligt for hinanden	28
38.14	Hvad er den hexadecimale notation for kommandoerne til at gøre følgende (husk at numre på registre og RAM celler angives hexadecimalt)	28
38.14.a	Kopiere indholdet af register C til RAM celle 0A. . . .	28
38.14.b	Lægge bitmønstret 10110011 ind i register 2.	29
38.14.c	Addere register 3 og 4, og lægge resultatet i register 5.	29
38.14.d	Lave bit-wise XOR af register B og C.	29
38.14.e	Hoppe til instruktionen i RAM celle 14 hvis indholdet i register C er større ($>$) end indholdet i register 0.	29
38.15	Forklar følgende kode	29
38.16	Lav et program som læser to heltal fra RAM cellerne 10 og 12, finder deres sum, og skriver resultatet i RAM celle 14. [Hint: det er en let forandring af det første eksempelprogram.]	29
38.17	Lav et program som læser et heltal k fra RAM celle 18 og som skriver summen $1+2+3+\dots+(k-1)$ i RAM celle E1. [Hint: det er en let forandring af det andet eksempelprogram.] Da man med 8 bits heltal i two's complement kun kan repræsentere heltal op til 127, skal vi have $k \leq 16$ for at kunne repræsentere resultatet.	30
38.18	Lav et program som læser to heltal fra RAM celle 16 og 18, og som skriver det største af dem i celle 14.	30
38.19	Lav et program som læser et heltal k fra RAM celle 20 og som skriver bitmønstret 11111111 (hexadecimalt: FF) i RAM celle 22 hvis k er forskellig fra 0, og skriver bitmønstret 01010101 (hexadecimalt: 55) i RAM celle 22 hvis k er lig 0	31

38.20	Lav et program som læser et bitmønster fra RAM celle 10, laver de første fire bits om til 0'er, og skriver svaret i RAM celle 12. Hint: det kan gøres med bit-wise AND med et bestemt bitmønster (hvilket?).	31
38.21	Lav et program som læser to bitmønster x og y fra RAM cellerne 20 og 22, laver et nyt bitmønster, som består af de første fire bits fra x efterfulgt af de sidste fire bits fra y, og skriver svaret i RAM celle 22. Hint: brug ideen fra sidste opgave to gange, samt bit-wise OR	32
38.22	Lav et program som læser to bitmønster x og y fra RAM cellerne 20 og 22, laver et nyt bitmønster, som består af de sidste fire bits fra y efterfulgt af de første fire bits fra x, og skriver svaret i RAM celle 22. Hint: brug ideen fra sidste opgave, samt cyklisk rotation af bits.	32
39	Uge	33
39.1	Løs opgaven fra sidste side i slides om CPU'er og maskinkode, dvs. lav et program som tæller ned i stedet for op. Mere præcist, lav et program som efter tur skriver tallene 6, 5, 4, 3, . . . , 0 (dvs. indhold 06, 05, 04, 03, . . . , 00) i RAM celle 1E, hvis RAM celle 18 indeholder 07 til at starte med.	33
39.2	I opgave II.12 fra uge 36/37 blev beskrevet følgende alternative metode til at skifte fortegn på heltal repræsenteret i two's complement: Invertér alle bits i tallet og læg derefter 1 til tallet. Implementer denne metode i et program. Mere præcist, lav et program som læser et heltal x (i two's complement) fra RAM celle 20 og skriver tallet $-x$ (i two's complement) i celle 22. [Hint: bits i x kan inverteres ved bitwise XOR af x med et bestemt bitmønster (hvilket?).]	34
39.3	Multiplikation	34
39.1	Er følgende en algoritme	35
39.2	Betragt listen $L = [1, 2, 3, 4, 5, 6, \dots, 20]$. I nedenst[ende spørgsmål tæller vi sammenligninger som involverer elementer i listen. . .	35
39.2.a	Hvor mange sammenligninger foretages der med SequentialSearch(L , 7)?	35
39.2.b	Hvor mange sammenligninger foretages der med BinarySearch(L , 7)?	35
39.2.c	Antag nu, at L indeholder 10.000 elementer. Hvor mange sammenligninger foretager man i værste tilfælde med en sekventiel søgning i L ?	36

39.2.d	Hvor mange sammenligninger foretager man i værste tilfælde med en binær søgning i L ?	36
39.3	Udfyld de manglende felter (undtagen dem i øverste række) i tabellen på side 11 i slides fra Lenes forelæsning	36
39.4	Hvilken af følgende udsagn er sande?	36
39.4.a	$n \in O(n)$	36
39.4.b	$2n + 5 \in O(n)$	36
39.4.c	$\sqrt{n} - \log(n) \in O(n)$	36
39.4.d	$(\log(n))^2 \in O(n \log n)$	37
39.4.e	$n^2 \in O(n)$	37
39.4.f	$n \in O(n^2)$	37
39.4.g	$n \log(n) \in O(n^2)$	37
39.4.h	$n \log(n) \in O(n)$	37
39.4.i	$3n^2 + 2n + 1 \in O(n^2)$	37
39.4.j	$3n^2 + 2n + 1 \in O(n)$	37
39.5	Angiv for hver af følgende algoritmer deres asymptotiske køretid i O -notation som funktion af n	37
39.5.a	Algoritme 1	38
39.5.b	Algoritme 2	38
39.5.c	Algoritme 3	38
39.5.d	Algoritme 4	38
39.6	Betragt følgende algoritme til at finde det mindste tal i listen L .	38
39.6.a	Hvad er algoritmens køretid	38
39.6.b	Opskriv en løkke-invariant for algoritmen og bevis at den altid finder det mindste lement i L	38
39.6.c	Omskriv algoritmen så den bruger en while-løkke i stedet for en for-løkke	38
39.6.d	Bemærk at algoritmen er iterativ skriv en rekursiv version af algoritmen	39
39.1	Hvilke af følgende udsagn er sande?	39
39.1.a	$n \in O(n^3)$	39
39.1.b	$n^3 \in O(n^2)$	39
39.1.c	$\log(n) \in O(n)$	39
39.1.d	$n \in O(n \log(n))$	39
39.1.e	$0.1n^2 + n + 10 \in O(n)$	39
39.1.f	$0.1n^2 + n + 10 \in O(n^2)$	40
39.1.g	$0.1n^2 + n + 10 \in O(n^3)$	40
39.1.h	$n^2 \log(n) \in O(n^2)$	40
39.2	Angiv for følgende algoritme dens asymptotiske køretid i O -notation som funktion af n	40

39.3	Husk på algoritmerne til, ciffer for ciffer, at addere eller gange to tal i hånden	40
39.3.a	Hvad er køretiden for at addere to tal med n cifre hver? Hvad er den karakteristiske operation?	40
39.3.b	Hvad er køretiden for at gange to tal med n cifre hver? Hvad er den karakteristiske operation?	40
40	Uge	41
40.1	Opskriv i pseudokode algoritmen Sequential Search ved hjælp af operationerne <code>readNext()</code> , <code>isEndOfFile()</code> , <code>open()</code> og <code>close()</code> fra interfacet sekventiel tilgang.	41
40.2	Opskriv i pseudokode algoritmen for merge af to lister ved hjælp af operationerne <code>readNext()</code> , <code>isEndOfFile()</code> , <code>writeNext(data)</code> , <code>open()</code> og <code>close()</code> fra interfacet sekventiel tilgang.	41
40.3	I denne opgaver repræsenterer vi mængder som sorterede lister uden dubletter. For eksempel vil de to mængder $A = \{5, 3, 9, 8\}$ og $B = \{3, 2, 9, 10, 27\}$ være repræsenteret som disse	lister:
	$A = [3, 5, 8, 9]$	
	$B = [2, 3, 9, 10, 27]$	
	Beskriv en algoritme til at beregne repræsentationen af forenings mængden $X \cup Y$ ud fra repræsentationen af to mængder X og Y	42
40.4	Beskriv en algoritme til at flette (merge) indholdet af tre sorterede lister A , B og C sammen til en sorteret liste D . Hvad er køretiden for din algoritme?	42
40.5	Givet en algoritme til at flette indholdet af tre sorterede lister A , B og C sammen til én sorteret liste D (dvs. givet en løsning til opgave 4), beskriv en variant af Mergesort baseret på denne. Hvad er køretiden for din algoritme?	42
40.6	Hvis en hashfunktion h er givet ved $h(x) = x \% 11$, på hvilke pladser i tabellen ender tallene 25, 75, 125, 175?	43
40.7	Hvis en hashfunktion h er givet ved $h(x) = x \% 11$, hvor mange pladser i hashtabellen har mere end ét element, når der indsættes elementerne 34, 65, 122 og 155?	43
40.8	Beregn med lommeregner svaret på følgende: Hvis 3 elementer indsættes tilfældigt i et array med 7 pladser, hvad er sandsynligheden for, at der ikke er to elementer som ender på samme plads?	43

40.9	Beregn med lommeregner følgende svaret på følgende: Hvis 5 elementer indsættes tilfældigt i et array med 12 pladser, hvad er sandsynligheden for, at der ikke er to elementer som ender på samme plads?	44
40.1	Hvis en hashfunktion h er givet ved $h(x) = x\%17$, på hvilke pladser i tabellen ender tallene 22, 72, 122, 172?	44
40.2	Hvis en hashfunktion h er givet ved $h(x) = x\%17$, hvor mange pladser i hashtabellen har mere end ét element, når der indsættes elementerne 40, 74, 101 og 159?	44
40.3	Lav et Java-program med input n og k der for situationen hvor n elementer indsættes tilfældigt i et array med k pladser finder sandsynligheden for, at der ikke er to elementer som ender på samme plads.	45
40.4	Hvis 1000 elementer indsættes tilfældigt i et array med 1.000.000 pladser, hvad er sandsynligheden for, at der ikke er to elementer som ende på samme plads?	45
40.5	Hvis n elementer indsættes tilfældigt i et array med 1.000.000 pladser, hvor stor skal n være for at sandsynligheden for, at der ikke er to elementer som ender på samme plads, bliver mindre end $\frac{1}{2}$	45
40.6	[Udfordrende] Beskriv en algoritme, der som input tager et tal K og to sorterede lister X og Y , hver med n tal, og finder ud af, om der findes et par at tal $x \in X$ og $y \in Y$ for hvilke $x + y = K$. Din algoritme skal køre i tid $O(n)$. Du skal argumentere for køretiden og for korrektheden af svaret. . . .	45
41	Uge	46
41.1	Exercise. k -Neares Neighbors: Prediction	46
41.2	Exercise. k -Nearest Neighbors: Prediction	46
41.3	Exercise. Linear Regression: Prediction	47
41.4	Exercise. Linear Regression: Training	48
41.5	Exercise. Logical Functions and Perceptrons	48
	41.5.a OR gate	49
	41.5.b NOT gate	49
	41.5.c Create NAND gate	49
41.6	Exercise. Multilayer Perceptrons	49
41.7	Exercise. Single Layer Neural Networks: Prediction	50
	41.7.a Calculate output with $\vec{x} = (5, 10)$ using step function .	50
	41.7.b Calculate output with $\vec{x} = (5, 10)$ using sigmoid function	50
	41.7.c Will the two functions always result in the same result, which one is more correct?	50

41.7.d	Make a plot with the predictions and find a line	51
41.8	Exercise. Expressivness of a single layer perceptron	51
41.1	Exercise. k 'Nearest Neighbors: Prediction	52
41.2	Exercise. k -Nearest Neighbors: Prediction	53
41.3	Exercise. Linear Regression: Training	53
41.4	Exercise. Feed-Forward Neural Network: Single Layer Percep- tron	54
41.5	Exercise. Single Layer Perceptrons	55
41.6	Exercis. Logical Functions and Neural Networks	55
43	uge	55
43.1	Beregn følgende	55
43.1.a	L_3 -normen af $\vec{v} = (-2, 5)$	55
43.1.b	L_7 -normen af $\vec{v} = (4.5, -3.2)$	55
43.1.c	L_1 -normen af $\vec{v} = (5, 9)$	56
43.1.d	$L_{1.5}$ -normen af $\vec{v} = (2, 3)$	56
43.1.e	L_∞ -normen af $\vec{v} = (4.5, -3.2)$	56
43.2	For $\vec{p} = (1, 2, 3)$ og $\vec{q} = (0, 5, -2)$ beregn følgende:	56
43.2.a	Afstanden $\text{dist}_2(\vec{p}, \vec{q})$	56
43.2.b	Afstanden $\text{dist}_3(\vec{p}, \vec{q})$	56
43.2.c	Afstanden $\text{dist}_1(\vec{p}, \vec{q})$	56
43.2.d	Afstanden $\text{dist}_\infty(\vec{p}, \vec{q})$	56
43.3	Forklar figuren mudt på side 18 i Melih Kandemirs slides. Dvs. forkalr hvorfor mængden af alle punkter \vec{q} i en given afstand r fra et punkt \vec{q} (også kaldet "cirklen" om \vec{q} med radius r) har en sådan facon, når afstanden er givet ved dis_1	57
43.3	Forklar også figuren til højre på samme side	57
43.3	Forsøg også at forklare, hvorfor L_∞ er et godt navn for max- normen, når man sammenligner med definitionen af L_p	57
43.4	Consider the five picture given in Figure 1 each with 36 pixels.	57
43.4.a	Extract from each picture a color histogram with the bins <i>red</i> , <i>orange</i> , and <i>blue</i> (the white pixels are ignored)	57
43.4.b	For each of the pictures a to d , calculate their similarity to q using Euclidean distance (i.e. using dist_2	58
43.5	Repetér definitionen af en centroide for en cluster C bestående af følgende tre punkter	59
43.6	Check beregningen af de to centroder i figuren på side 32	59
43.7	Consider the following data set (with 8 objects in \mathbb{R}^2) used in the lecture:	59
43.7.a	Compute a complete partitioning with $k = 2, 3, 4, 5$ using k means method	60

43.8	Repetet forskellen på Forgys-Lloyds og MacQueens udgaver af k-means algoritmen, giver de to udgaver altid samme resultat.	60
44	Uge	60
44.1	Exercise	60
44.2	Exercise	61
44.3	Exercise	61
44.4	Exercise	61
44.5	Exercise	61
44.6	Exercise	62
44.7	Exercise	62
44.8	Exercise	63
44.9	Exercise	63
44.10	Exercise	63
44.11	Exercise	64
45	uge	64
45.1	Prove that the best online algorithm for the ski problem has a competitive ratio on $\frac{19}{10}$	64
45.2	For the schedule algorithm, what are the result of $m = 3$. . .	65
45.3	Make input for any algorithm with $m = 2$ which will result in better result than $\frac{3}{2}$ of the optimum	65
45.4	Show that the following data can be in three bins	65
45.5	Use First Fit on the following data, where the max size is 6 . .	66
45.6	Why can the following result not be amde by First Fit, max size is 9	67
45.1	Find a squence where Ff performs $\frac{5}{3}$ times worse than OPT . .	67
46	Uge	67
46.1	Which of the following formulas are satisfiable	67
46.1.a	$A \wedge B$	67
46.1.b	$A \vee B$	67
46.1.c	$A \rightarrow B$	68
46.1.d	$A \wedge \neg A$	68
46.1.e	$A \vee \neg A$	68
46.2	Which if the following formulas are equivalent (same assignment satisfy)	68
46.3	Convert the following formulas into CNF	68
46.3.a	$\neg A \wedge B$	68
46.3.b	$\neg A \vee B$	68
46.3.c	$A \rightarrow B$	68

46.3.d	$(A \rightarrow B) \wedge (\neg B \rightarrow A)$	68
46.4	Breaking symmetry in N-Towers and N-Queens	69
46.4.a	Write two clauses that forbid solutions where there is a queen in the irght half of the first row	69
46.4.b	Instead of adding two clauses change an existing clause	69
46.6	The formula from Slide 11 contains redundant information. FOr Example $X_{1,1} \rightarrow \neg X_{1,2}$ and $X_{1,2} \rightarrow \neg X_{1,1}$ are equivalent. Understand and remove these redundancies:	69
46.6.a	Why do these redundancies occur?	69
46.6.b	Identify all such redundacies!	69
46.6.c	Write down a simplified formula without redundancies	69
46.6.d	Convert the formula to CNF	69
46.6.e	Write the formula in DIMACS format	69
46.6.f	Run it in a SAT and test result	70
46.1	Which of the following formulas are satisfiable	70
46.1.a	$(A \rightarrow B) \wedge (B \rightarrow A)$	70
46.1.b	$(A \rightarrow B) \wedge (B \rightarrow A) \wedge A$	70
46.1.c	$(A \rightarrow B) \wedge (B \rightarrow A) \wedge \neg A$	70
46.1.d	$(A \rightarrow B) \wedge (B \rightarrow A) \wedge (\neg A \rightarrow \neg B) \wedge (\neg B \rightarrow A)$	70
46.2	Whuch of the following formulas are equivalent	70
46.3	Convert to CNF	71
46.3.a	$(\neg A \rightarrow B) \wedge (\neg B \rightarrow \neg A)$	71
46.3.b	$A \rightarrow (\neg(B \wedge D))$	71
46.3.c	$A \rightarrow (\neg(B \vee D))$	71
46.3.d	$A \rightarrow (\neg(B \rightarrow (C \wedge D)))$	71
47	47	71
47.1	Given the follwing relation schema:	71
47.2	The relation schema of task 1 together with the vald tuples define a relation instance. Visualize this relation instance as a table	72
47.3	Given the following relation instance	72
47.4	Given the following Entity-Relationship diagram	72
47.5	You are given the relation instance defined in task 3	73
47.6	You are given the following ER-diagram:	73
47.7	Specify an SQL command that deletes formthe Moveis table all moeis that were not produced in 1994	74
47.8	You want to retrive the titles f all moveis from the Moviestable of task3 that were produced in 1994 and directed by Quentin Tarantino. Express the query in bth theese ways:	74

47.9	Consider the Movies table of task 3. Provide in SQL one INSERT and one DELETE command that can to be executed to change it into the following table	75
47.10	Specify an SQL command withot set operations (UNION or EXCEPT) that retirves all movies from the Movie table, that have been produced before 1990 or that have a budget of at least 30 million USD. State the same query as an relational algebra expression	75
47.11	Solve task 10 with SQL operations (UNION OR EXCEPT). State the same query as an relational algebra expression. . . .	75
47.12	Specify an SQL command without set operations (UNION or EXCEPT) that retrieves all movies from the Movie table if task 3 that either	76
47.13	Specify an SQL command that retireves all pairs of movies from the Movies table fo task 3 that have been directed by the same director.	76
47.14	Specify an SQL command that retrieves all pairs of mvoes (move1, movie2) from the Movies table fo task 3 with movie1's budget exceeding the budget if movie2	76
47.1	Which of the following statements are true?	77
47.2	Joins are compound operator which we did not cover in the lcture. They are useful for joining (combining) the data contained in muliple relations together. In relaional algebra the conditional join operator \bowtie_C (also called the θ -join operator) is defined by	77
47.3	Specify an SQL command that calculates hte conditional join given in task 2	78
47.4	Specify an SQL command that calculates the following nested relational operation involving two conditional joins	78
48	Uge	78
48.1	Suppose in RSA the public key is $PK = (1517, 13)$. Which of the following is the RSA encryption if the message 43	78
48.2	Is one of the following the multiplicative inverse if 49 modulo 221	78
48.3	Which of the following sets of public key (OK) and secret key (SK) is a valid set of RSA keys (igoring the numbers are not large eneenough)	79
48.3.a	$PK = (91, 37); SK = (91, 23)$	79
48.3.b	$PK = (143, 77); SK = (143, 53)$	79
48.3.c	$PK = (231, 59); SK = (231, 47)$	79

48.3.d	$PK = (107, 25); SK = (107, 30)$	79
48.4	In the Sieve of Eratosthenes, how many lists have been created at the point where the number 13 is the first element in the list?	79
48.5	Consider an RSA system with Alice's public key $n = 1517$ and $e = 17$. Note that $1517 = 37 \cdot 41$	79
48.5.a	Find Alice's secret key d . Use the extended Euclidean Algorithm from page 42 of the slides from the lecture	79
48.5.b	Try encrypting 423. Use the algorithm for fast modular exponentiation. How many times during the recursive execution is the <i>if</i> k is odd case encountered?	80
48.5.c	Decrypt the number obtained above, how many times odd and even?	80
48.6	Why is cryptographically secure hash function used in connection with RSA digital signatures?	80
48.7	With RSA why would you never use the value 2 as one of the two primes p and q	80
48.8	In RSA why must the message being encrypted be a non-negative integer strictly less than the modulus	80
48.1	Try breaking these two encrypted messages	80
48.1.a	Caesar cipher in english	80
48.1.b	Decrypt mono-alphabetic cipher	81
49	Uge	81
49.1	Why in RSA is it necessary that $\gcd(e_A, (p_A - 1)(q_A - 1)) = 1$?	81
49.2	Draw the graph representing the road system in the figure below, and write down the number of vertices, the number of edges and the degree of each vertex	81
49.3	On Twitter:	81
49.3.a	John follows Joan, Jean and Jane; Joe follows Jane and Joan; Jean and Joan follow each other. Draw a diagram illustrating these follow relationships between John, Joan, Jane and Joe.	81
49.3.b	Twitter has 313 million active users (June 2016, based on Twitter Inc.) Imagine you would like to store the diagram for the follow relationships in an adjacency matrix that uses 4 bytes per entry on your new laptop which has 64 gb of RAM. Is this feasible	82

49.3.c	The municipality of Odense has a population of 200000 people. Let G be the graph where the meaning of an edge from vertex i to j is "person i is friends with person j ". Imagine you would like to store the adjacency matrix for this graph for the relationships in a matrix representation that uses 4 bytes per entry on your new lapto which has 64 GB of RAM. Is this feasible?	82
49.4	Consider the following six graphs (note tat the nodes do not have labels).	82
49.4.a	How many walks of length 3 formthe red vertex to the green vvertex are there in graph 3?	82
49.4.b	How many paths from the red vertex to the green vertex are there in graph 3	83
49.4.c	How many shortest paths from the red vertex to the green vertex are there in graph 3?	83
49.4.d	For each of the graphs: what is the longest of all pairwise shortest paths?	83
49.4.e	Give an adjacency matrix for graph 1. Can there be different adjaccency matrices for the same graph? If so name a second adjacency matrix for graph 1. Can you find two different adjacency matrices for graph 6? . . .	83
49.5	Let A be an adjacency matrix. In the lecture you learned that the ij -entry of A^k is the number of different walks from vertex i to vertex j using exactly k edges	84
49.5.a	What is the interpretation of ij -entry of the matrix $A^1 + A^2 + A^3$?	84
49.5.b	Complete the following sentence with the missing expression: In a graph G with adjacency matrix A , vertex i and j are connected if and only if $... > 0$	84
49.1	Find four different square roots of 1 modulo 143, i.e., numbers which multiplied by themselves modulo 143 give 1 (and which are at least 0 and less than 143). You may consider writing a simple program for finding them.	84
49.2	Try executing the Miller-Rabin primality test on 11, 15, and 561.	84
49.2.a	What types of numbers are they?	84
49.2.b	Which numbers showed it was a composit?	84
50 Uge		85
50.1	Let the following weighted graph G (from the lecture slides, weights are depicted in red) be given:	85

50.1.a	How many shortest path in G are of length 6? Name them.	85
50.1.b	How long is the longest of all pairwise shortest paths in the graph? Are there several longest shortest paths?	85
50.1.c	How many paths in G are of length 6? (Note: a path does not necessarily need to be a shortest path.) Name them.	85
50.2	Assume in this exercise that all weights on edges are non-negative values.	86
50.2.a	In a graph G with $n = 6$ vertices, how man matrix-matrix multiplication operations are needed in the worst case in order to compute the distance matrix D , when the method of repeated squaring is used to compute D	86
50.2.b	In a graph G with $n = 200$ vertices, how many matrix-matrix multiplications are needed in the worst case in order to compute the distance matrix D , when the method of repeated squaring is used to compute D ?	86
50.2.c	Can yopu find a graph G with $n = 6$ vertices for which $W^4 \neq W^5$? if so depict it	86
50.2.d	Can yopu find a graph G wit hn = 6 vertices for which $W^5 \neq W^6$? if so depict it	87
50.2.e	Can yopu find a graph G wit hn = 6 vertices for which $W^1 = W^2$? if so depict it	87
50.2.f	What is the computational runtime in order to compute the distance matrix D for a graph G with n vertices if the method of repeated squaring is used to compute D ?	88
50.3	Consider the following molecule (it's called 2,3-Dimethylhexane	88
50.3.a	How many carbon atoms does this molecule have?	88
50.3.b	Draw the graph G corresponding to the carbon backbone of the molecule	89
50.3.c	Give the edge weight matrix W for the graph G	89
50.3.d	Use your brain or the Java program ShortestPaths.java to infer the distance matrix.	90
50.3.e	What is the Wiener Index $W(G)$	90
50.3.f	How many shortest paths of length $3i \rightarrow \dots \rightarrow j$ with $i < j$ are in G	90
50.3.g	Using Wiener's method for predicting the boiling point, what is your prediction for 2,3-Dimethylhexane?	90

50.4 Assume in this exercise that all weights on edges are non-negative values. Prove the following theorem stated on the slides	90
--	----

36 Uge

36.1 Konvertér følgende tal i 2-talsystemet (binær repræsentation) til 10- talsystemet

$$101_2 \rightarrow 5_{10}$$

$$101011_2 \rightarrow 43_{10}$$

$$111111_2 \rightarrow 63_{10}$$

36.2 Konvertér følgende tal i 3-talsystemet til 10-talsystemet

$$212_3 \rightarrow 2 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 = 2 + 3 + 18 = 23_{10}$$

$$20102_3 \rightarrow 2 \cdot 3^0 + 0 \cdot 3^1 + 1 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 = 2 + 9 + 162 = 173_{10}$$

36.3 Konvertér følgende hexadecimale udtryk, set som tal i 16-talsystemet, til tal i 10-talsystemet

$$C_{16} \rightarrow 12_{10}$$

$$1A_{16} \rightarrow 10 + 16 \cdot 1 = 26_{10}$$

$$F05_{16} \rightarrow 15 + 16^2 + 5 = 3845_{10}$$

36.4 Konvertér følgende hexadecimale udtryk til bitstreng

$$2_{16} \rightarrow 10_2$$

$$A1_{16} \rightarrow 10100001_2$$

$$FF05_{16} \rightarrow 111111110101_2$$

36.5 Konvertér følgende bitstreng til hexadecimale udtryk

$$1110_2 \rightarrow E_{16}$$

$$10101110_2 \rightarrow AE_{16}$$

$$0001111010111111_2 \rightarrow 1DBF_{16}$$

36.6 Lav følgende additioner i 2-talsystemet (binær repræsentation)

$$\begin{array}{rcccc} & 1 & 0 & 1 & 1_2 \\ + & & 1 & 1 & 0_2 \\ \hline 1 & 0 & 0 & 0 & 1_2 \end{array}$$

$$\begin{array}{rcccccc} & 1 & 1 & 1 & 0 & 1 & 0_2 \\ + & & 1 & 1 & 0 & 1 & 1_2 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 & 1_2 \end{array}$$

36.7 Konvertér følgende tal i 10-talsystemet til 2-talsystemet (binær repræsentation)

$$\begin{aligned} 21_{10} &\rightarrow 10101_2 \\ 63_{10} &\rightarrow 111111_2 \\ 101_{10} &\rightarrow 1100101_2 \end{aligned}$$

36.8 Konvertér følgende tal i 10-talsystemet til 3-talsystemet

$$\begin{aligned} 21_{10} &\rightarrow 210_3 \\ 101_{10} &\rightarrow 10202_3 \end{aligned}$$

36.9 Konvertér følgende tal i two's complement (8 bits) til 10-talsystemet

$$\begin{aligned} 10101010_2 &\rightarrow -128 + 2 + 8 + 32 = -86_{10} \\ 01010101_2 &\rightarrow 1 + 4 + 16 + 64 = 85_{10} \end{aligned}$$

36.10 Vend fortegnet på følgende tal i two's complement (8 bits)

$$\begin{aligned} 10110000_2 &\rightarrow 01010000_2 \\ 01010101_2 &\rightarrow 10101011_2 \end{aligned}$$

36.11 Konvertér følgende tal i 2-talsystemet med fast decimalpunkt til 10 talsystemet

$$11.101_2 \rightarrow (2^1 + 2^0) \cdot (2^{-1} + 2^{-3}) = 3\frac{5}{8}$$
$$1101.10101_2 \rightarrow (2^0 + 2^2 + 2^3) \cdot (2^{-1} + 2^{-3} + 2^{-5}) = 13\frac{21}{32}$$

36.12 Konvertér følgende tal i 2-talsystemet fra fast decimalpunkt til flyden- de decimalpunkt (med notationen fra slides for 8 bits flydende decimalpunktstal)

$$-0.00101_2 \rightarrow 1|111|0100$$
$$1100.0 \rightarrow 0|011|1000$$

37 Uge

37.1 Konvertér følgende tal i 2-talsystemet (binær repræsentation) til 10-talsystemet

$$10101101_2 \rightarrow 1 + 4 + 8 + 32 + 128 = 173_{10}$$
$$11111100_2 \rightarrow 4 + 8 + 16 + 32 + 64 + 128 = 252_{10}$$

37.2 Konvertér følgende tal i 3-talsystemet til 10-talsystemet

$$1212_3 \rightarrow 2 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 + 1 \cdot 3^3 = 2 + 3 + 18 + 27$$
$$= 40_{10}$$
$$111111_3 \rightarrow 1 \cdot 3^0 + 1 \cdot 3^1 + 1 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4 + 1 \cdot 3^5 + 1 \cdot 3^6$$
$$= 1 + 3 + 9 + 27 + 81 + 243 = 364_{10}$$

37.3 Konvertér følgende hexadecimale udtryk, set som tal i 16-talsystemet, til tal i 10-talsystemet

$$A5B2_{16} \rightarrow 2 \cdot 16^0 + 11 \cdot 16^1 + 5 \cdot 16^2 + 10 \cdot 16^3$$
$$= 2 + 176 + 1280 + 40960 = 42418_{10}$$

37.4 Konvertér følgende hexadecimale udtryk til bitstreng

$$CAB_{16} \rightarrow 1100|1010|1011_2$$
$$001A_{16} \rightarrow 1|1010$$

37.5 Konvertér følgende bitstreng til hexadecimalt udtryk

$$1010|0101|1101 \rightarrow A5D$$

37.6 Lav følgende additioner i 2-talsystemet (binær repræsentation)

$$\begin{array}{r} 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1_2 \\ + \quad \quad \quad \quad \quad 1_2 \\ \hline 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0_2 \end{array}$$

$$\begin{array}{r} 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1_2 \\ + \quad \quad \quad \quad \quad 1_2 \\ \hline 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0_2 \end{array}$$

37.7 Konvertér følgende tal i 10-talsystemet til 2-talsystemet (binær repræsentation)

$$117_{10} \rightarrow 1110101_2$$
$$256_{10} \rightarrow 100000000_2$$
$$2345_{10} \rightarrow 100100101001$$

37.8 Konvertér følgende tal i 10-talsystemet til 3-talsystemet

$$789_{10} \rightarrow 1002020_3$$

37.9 Konvertér følgende tal i two's complement (8 bits) til 10-talsysteme

$$00110110_2 \rightarrow 54_{10}$$
$$11110010_2 \rightarrow -256 + 2 + 16 + 32 + 64 = -14_{10}$$

37.10 Vend fortegnet på følgende tal i two's complement (8 bits)

$$00111000_2 \rightarrow 11001000_2$$

$$11110010_2 \rightarrow 00001110_2$$

37.11 Konvertér følgende tal i 10-talsystemet til 8 bits two's complement

$$-53_{10} \rightarrow 1001001_2$$

$$-126_{10} \rightarrow 10000010_2$$

37.12 På slides om repræsentation af tal er der angivet en metode til at skifte fortegn på heltal repræsenteret i two's complement. Her er en anden metode. Inverter alle bits i tallet og læg derefter 1 til tallet. Find et argument for, at de to metoder gør det samme. Forklar argumentet klarest muligt for hinanden

Ved at invetere efter det første bit vil det være ækvivalent til at invetere alt og tilføje 1 bit.

37.13 Konvertér følgende tal i 2-talsystemet med fast decimalpunkt til 10-talsystemet

$$101.111_2 \rightarrow 5.\frac{7}{8}$$

37.14 Konvertér følgende tal i 2-talsystemet fra fast decimalpunkt til flydende decimalpunkt - 8 bits notation

$$0.0001101_2 \rightarrow 0|100|1010$$

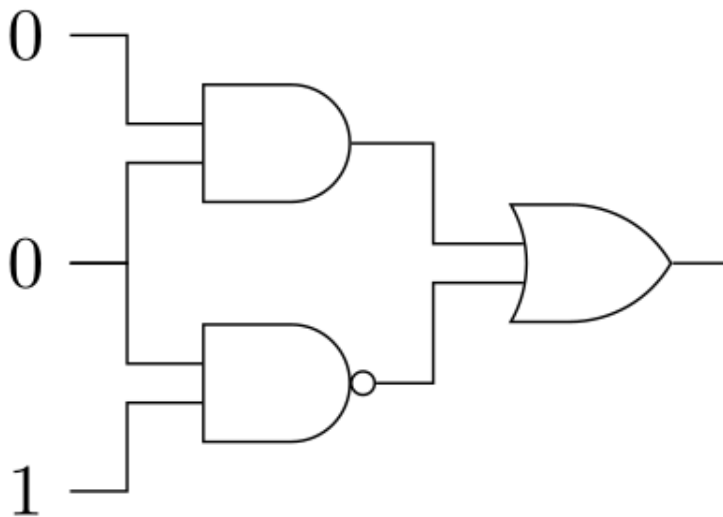
$$-1010.0_2 \rightarrow 1|011|0100$$

37.15 Konvertér følgende tal i flydende decimalpunkt (med notationen fra slides for 8 bits flydende decimalpunktstal) til 2-talsystemet med fast decimalpunkt, og derefter til 10-talssystemet

$$\begin{aligned} 0|111|0101 &\rightarrow 0.10101_2 \rightarrow 0.65625_{10} \\ 1|000|1100 &\rightarrow -1.1100 \rightarrow -1.75 \end{aligned}$$

38 Uge

38.1 Hvad er output af kredsløbet nedenfor?

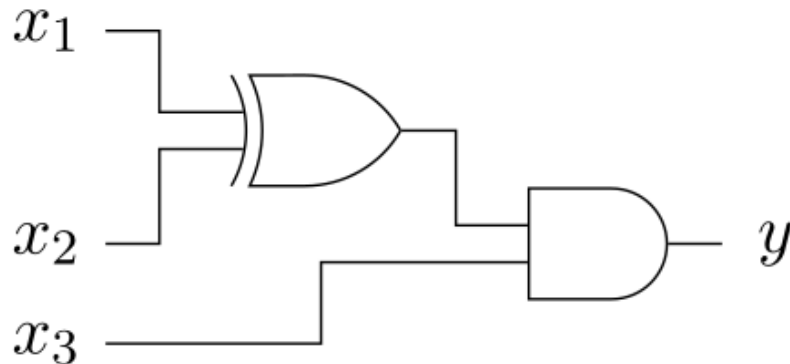


and - 0
nand - 1
or - 1

38.2 Hvad er værdien af nedenstående Boolske udtryk hvis (x_1, x_2, x_3) er lig $(0, 1, 0)$? Opskriv et kredsløb svarende til udtrykket. $(x_1 \wedge x_2) \oplus (x_3 \vee (\neg x_1))$

Venstre parentes giver 0 og højre giver 1 dermed giver den 1.

38.3 Opskriv et Boolsk udtryk om svarer til nedenstående kredsløb. For hvilke værdier af x , y og z vil kredsløbet kredsløbet nedenfor give output 1? Opskriv hele tabellen for kredsløbet.



$$(x_1 \oplus x_2) \wedge x_3$$

x_1	x_2	x_3	$x_1 \oplus x_2$	$x_3 \wedge (x_1 \oplus x_2)$
1	1	1	0	0
1	1	0	0	0
1	0	1	1	1
1	0	0	1	0
0	1	1	1	1
0	1	0	1	0
0	0	1	0	0
0	0	0	0	0

38.4 Lav et Boolsk udtryk med NOT, AND, OR og tre input variable, som har nedenstående tabel. Tegn også et tilsvarende kredsløb med tre inputs.

$$(\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge x_3)$$

x_1	x_2	x_3	y
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

38.5 Vis hvordan man kan lave en OR-gate ved hjælp af AND-gates og NOT-gates. (Til forelæsningen blev det vist, at alle boolske funktioner kan implementeres med AND-, OR-, og NOT-gates. Opgaven her viser, at AND- og NOT-gates er nok.)

$$\neg(\neg x_1 \wedge \neg x_2) \rightarrow x_1 \vee x_2$$

38.6 Vis hvordan man kan lave en NOT-gate ved hjælp af en NAND-gate. Vis derefter hvordan man kan lave en AND-gate ved hjælp af NAND-gates. (Sammen med opgaven ovenfor viser dette, at NAND-gates er nok til at implementere alle boolske funktioner.)

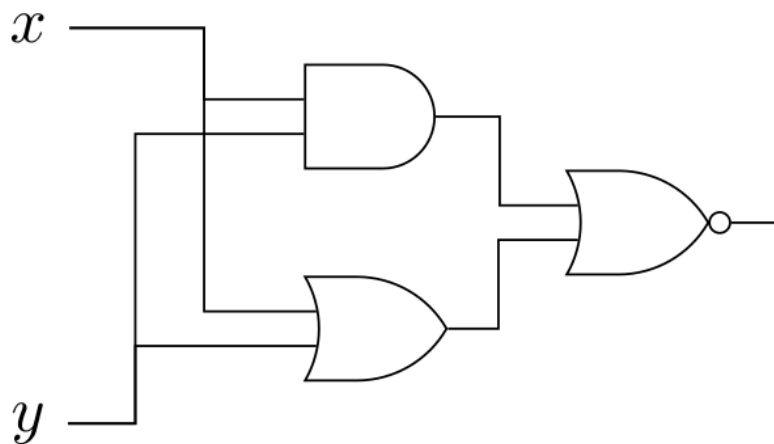
$$x_1 \neg \wedge x_1 \rightarrow \neg x_1$$

$$(x_1 \neg \wedge x_1) \neg \wedge (x_2 \neg \wedge x_2) \rightarrow x_1 \wedge x_2$$

x_1	x_2	x_3	y
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

38.7 [Repetition fra forelæsningen.] Opskriv den korrekte tabel for funktionen Resultat(x_1 , x_2 , x_3) fra slides om gates.

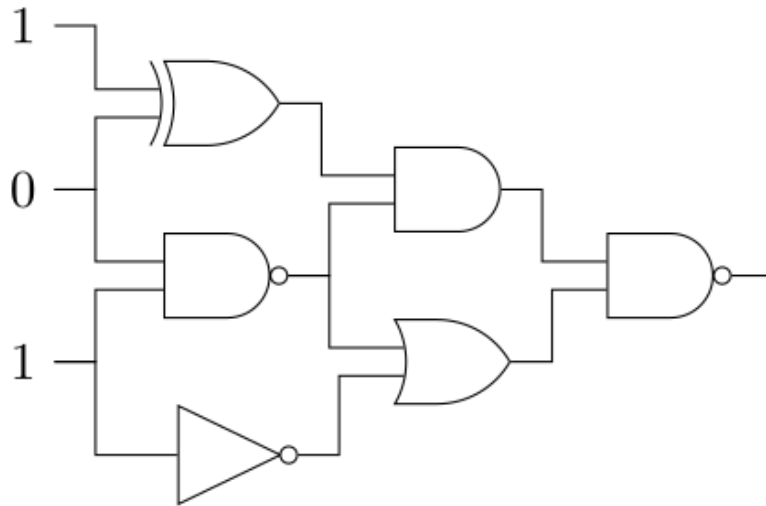
38.8 Opskriv tabellen for nedenstående kredsløb. Hvilken enkelt-gate svarer det til?



nand gate

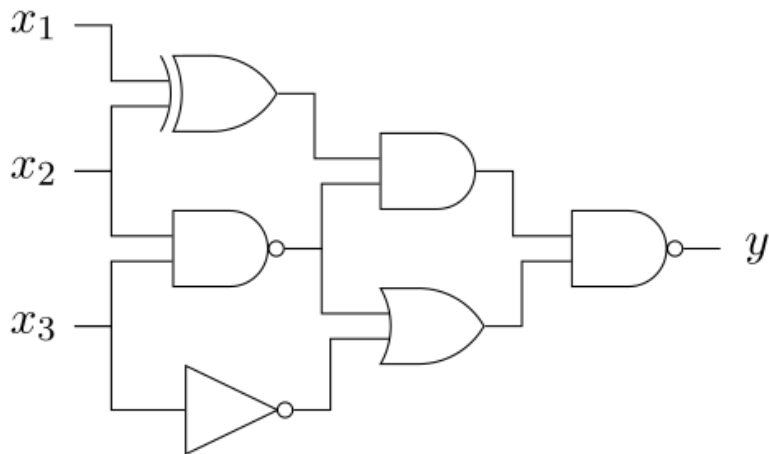
x	y	output
1	0	0
0	0	1
1	1	0
0	1	0

38.9 Hvad er output af kredsløbet nedenfor?



1 1 1
0 1 — 0
1 0 1

38.10 Opskriv et Boolsk udtryk som svarer til samme kredsløb. Opskriv hele tabellen for kredsløbet.



$$\neg(((x_1 \oplus x_2) \wedge \neg(x_2 \wedge x_3)) \wedge (\neg(x_2 \wedge x_3) \vee \neg x_3))$$

x_1	x_2	x_3	y
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

38.11 Lav et Boolsk udtryk med NOT, AND, OR og tre input variable, som har nedenstående tabel. Tegn også et tilsvarende kredsløb med tre inputs.

x_1	x_2	x_3	y
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

$$(\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3) \\ (\neg x_1 \wedge \neg x_2) \vee (x_1 \wedge \neg x_3)$$

38.12 [Repetition fra forelæsningen.] Opskriv den korrekte tabel for funktionen $\text{Mente}(x_1, x_2, x_3)$ fra slides om gates.

38.14.b Lægge bitmønstreet 10110011 ind i register 2.

22b3

38.14.c Addere register 3 og 4, og lægge resultatet i register 5.

6534

38.14.d Lave bit-wise XOR af register B og C.

9BBC XOR resultatet ligges i *B*

38.14.e Hoppe til instruktionen i RAM celle 14 hvis indholdet i register C er større ($>$) end indholdet i register 0.

DC14

38.15 Forklar følgende kode

1110
1212
5112
1214
5112
3118
C000

Koden tager data fra celle 10 og 12 og addere dem sammen i register 1 og nulstiller register 2.

38.16 Lav et program som læser to heltal fra RAM cellerne 10 og 12, finder deres sum, og skriver resultatet i RAM celle 14. [Hint: det er en let forandring af det første eksempelprogram.]

Her skal 1214 ændres til 3114

- 38.17** Lav et program som læser et heltal k fra RAM celle 18 og som skriver summen $1 + 2 + 3 + \dots + (k - 1)$ i RAM celle E1. [Hint: det er en let forandring af det andet eksempelprogram.] Da man med 8 bits heltal i two's complement kun kan repræsentere heltal op til 127, skal vi have $k \leq 16$ for at kunne repræsentere resultatet.

2000

2101
1518
301E
5404
5001
D506
C000
0000
0000
0000
0000
0800
0000
0000
0700

- 38.18** Lav et program som læser to heltal fra RAM celle 16 og 18, og som skriver det største af dem i celle 14.

1016
1118
D10A
3014
C000
3114
C000
0000
0000

0000
0500
0500
0400

- 38.19 Lav et program som læser et heltal k fra RAM celle 20 og som skriver bitmønsteret 11111111 (hexadecimalt: FF) i RAM celle 22 hvis k er forskellig fra 0, og skriver bitmønsteret 01010101 (hexadecimalt: 55) i RAM celle 22 hvis k er lig 0

100c
1120
B108
3222
C000
3355
C000
0100

- 38.20 Lav et program som læser et bitmønster fra RAM celle 10, laver de første fire bits om til 0'er, og skriver svaret i RAM celle 12. Hint: det kan gøres med bit-wise AND med et bestemt bitmønster (hvilket?).

1010
110E
8010
3012
3355
C000
0000
0F00
FF00

- 38.21** Lav et program som læser to bitmønster x og y fra RAM cellerne 20 og 22, laver et nyt bitmønster, som består af de første fire bits fra x efterfulgt af de sidste fire bits fra y, og skriver svaret i RAM celle 22. Hint: brug ideen fra sidste opgave to gange, samt bit-wise OR

1020
1122
1216
1318
8003
8112
7010
3022
C000
0000
0000
0F00
F000
0000
0000
0000
C800
9900

- 38.22** Lav et program som læser to bitmønster x og y fra RAM cellerne 20 og 22, laver et nyt bitmønster, som består af de sidste fire bits fra y efterfulgt af de første fire bits fra x, og skriver svaret i RAM celle 22. Hint: brug ideen fra sidste opgave, samt cyklisk rotation af bits.

1020
1122
1216
1318
8003

8112
7010
3022
C000
0000
0000
F000
0F00
0000
0000
0000
C800
9900

39 Uge

- 39.1 Løs opgaven fra sidste side i slides om CPUer og maskinkode, dvs. lav et program som tæller ned i stedet for op. Mere præcist, lav et program som efter tur skriver tallene 6, 5, 4, 3, . . . , 0 (dvs. indhold 06, 05, 04, 03, . . . , 00) i RAM celle 1E, hvis RAM celle 18 indeholder 07 til at starte med.

1018
1118
1216
5002
301E
B40E
D106
C000
0000
0000
0000
FF00
0700

39.2 I opgave II.12 fra uge 36/37 blev beskrevet følgende alternative metode til at skifte fortegn på heltal repræsenteret i two's complement: Invertér alle bits i tallet og læg derefter 1 til tallet. Implementer denne metode i et program. Mere præcist, lav et program som læser et heltal x (i two's complement) fra RAM celle 20 og skriver tallet $-x$ (i two's complement) i celle 22. [Hint: bits i x kan inverteres ved bitwise XOR af x med et bestemt bitmønster (hvilket?).]

1020

111E
2201
9001
3022
6020
C000
0000
0000
0000
0000
FF00
0700
0000
0000
FF00
0C00
F300

39.3 Multiplikation

1134
1236
2701
2300
2800
8571

5777
2A01
3313
A501
2600
B522
5626
500A
D318
5886
533A
4070
B10A
D10A
C000
0200
0500

39.1 Er følgende en algoritme

```
i=0  
while i != 5  
    i=i+2
```

Nej denn terminere ikke

39.2 Betragt listen $L = [1, 2, 3, 4, 5, 6, \dots, 20]$. I nedenst[ende spørgsmål tæller vi sammenligninger som involverer elementer i listen.

39.2.a Hvor mange sammenligninger foretages der med `SequentialSearch(L, 7)`?

7

39.2.b Hvor mange sammenligninger foretages der med `BinarySearch(L, 7)`?

3 - 10, 5, 7

39.2.c Antag nu, at L indeholder 10.000 elementer. Hvor mange sammenligninger foretager man i værste tilfælde med en sekventiel søgning i L ?

10.000

39.2.d Hvor mange sammenligninger foretager man i værste tilfælde med en binær søgning i L ?

$$\frac{\frac{\ln n}{\ln 2}}{\ln 2} = 14$$

39.3 Udfyld de manglende felter (undtagen dem i øverste række) i tabellen på side 11 i slides fra Lenes forelæsning

Mængden af operationer udført på en given tid med en givet O nationen.

$$10^{\frac{9}{10}} \cdot 1s = \log_2(n)$$

$$n = 4.6 \cdot 10^{3000000000}$$

	1ms	1s	1min	1 day	1 year
$\log_2 n$	$10^{300,000}$	$4.6 \cdot 10^{3000000000}$	∞	∞	∞
n	10^6	10^9	$6 \cdot 10^{10}$	$9 \cdot 10^{13}$	$3 \cdot 10^{16}$
$n \log_2 n$	$6 \cdot 10^4$	$4 \cdot 10^7$	$2 \cdot 10^9$	$2 \cdot 10^{12}$	$6 \cdot 10^{14}$
n^2	10^3	32000	250000	$9 \cdot 10^6$	$2 \cdot 10^8$
n^3	10^2	10^3	$4 \cdot 10^3$	$4 \cdot 10^4$	$3 \cdot 10^5$
2^n	20	30	36	46	55

39.4 Hvilken af følgende udsagn er sande?

39.4.a $n \in O(n)$

True

39.4.b $2n + 5 \in O(n)$

True

39.4.c $\sqrt{n} - \log(n) \in O(n)$

True

39.4.d $(\log(n))^2 \in O(n \log n)$

True

39.4.e $n^2 \in O(n)$

False

39.4.f $n \in O(n^2)$

True

39.4.g $n \log(n) \in O(n^2)$

True

39.4.h $n \log(n) \in O(n)$

False

39.4.i $3n^2 + 2n + 1 \in O(n^2)$

True

39.4.j $3n^2 + 2n + 1 \in O(n)$

False

39.5 Angiv for hver af følgende algoritmer deres asymptotiske køretid i O -notation som funktion af n

```
ALGORITME1( $n$ )  
   $s = 0$   
  for  $i = 1$  to  $n$   
     $s = s + 1$   
  return  $s$ 
```

```
ALGORITME2( $n$ )  
   $s = 0$   
  for  $i = 1$  to  $n$   
    for  $j = 1$  to  $n$   
       $s = s + 1$   
  return  $s$ 
```

```
ALGORITME3( $n$ )  
   $s = 0$   
  for  $i = 1$  to  $n$   
    for  $j = i$  to  $n$   
       $s = s + 1$   
  return  $s$ 
```

```
ALGORITME4( $n$ )  
   $s = 0$   
  for  $i = 1$  to  $n$   
    for  $j = 1$  to  $n$   
      if  $i == j$   
        for  $k = 1$  to  $n$   
           $s = s + 1$   
  return  $s$ 
```

39.5.a Algoritme 1

$O(n)$

39.5.b Algoritme 2

$O(n^2)$

39.5.c Algoritme 3

$O(n^2)$

39.5.d Algoritme 4

$O(n^2)$

39.6 Betragt følgende algoritme til at finde det mindste tal i listen L .

```
Min(L)
n = L.length
min = L[1]
For i = 2 to n
    If L[i] < min
        min = L[i]
return min
```

39.6.a Hvad er algoritmens køretid

$O(n)$

39.6.b Opskriv en løkke-invariant for algoritmen og bevis at den altid finder det mindste lement i L

$x \geq \min$ for n

39.6.c Omskriv algoritmen så den bruger en while-løkke i stedet for en for-løkke

```

Min(L)
n = L.length
min = L[1]
i=2
while(i<=n)
    If L[i] < min
        min = L[i]
    i++
return min

```

39.6.d Bemærk at algoritmen er iterativ skriv en rekursiv version af algoritmen

```

Min(L, i, min)
n = L.length
If i<=n
    If L[i] < min
        min = L[i]
    return Min(L, i+1, min)
return min

```

39.1 Hvilke af følgende udsagn er sande?

39.1.a $n \in O(n^3)$

True

39.1.b $n^3 \in O(n^2)$

False

39.1.c $\log(n) \in O(n)$

True

39.1.d $n \in O(n \log(n))$

True

39.1.e $0.1n^2 + n + 10 \in O(n)$

False

39.1.f $0.1n^2 + n + 10 \in O(n^2)$

True

39.1.g $0.1n^2 + n + 10 \in O(n^3)$

True

39.1.h $n^2 \log(n) \in O(n^2)$

False

39.2 Angiv for følgende algoritme dens asymptotiske køretid i O -notation som funktion af n

```
s = 0
for i = 1 to n
    for j = i to n
        for k = i to j
            s = s + 1
return s
```

$O(n^3)$

39.3 Husk på algoritmerne til, ciffer for ciffer, at addere eller gange to tal i hånden

39.3.a Hvad er køretiden for at addere to tal med n cifre hver?
Hvad er den karakteristiske operation?

$O(n)$ Der sker en lille addition mellem hvert ciffer med de to tal og mende

39.3.b Hvad er køretiden for at gange to tal med n cifre hver?
Hvad er den karakteristiske operation?

$O(n^2)$

40 Uge

40.1 Opskriv i pseudokode algoritmen Sequential Search ved hjælp af operationerne `readNext()`, `isEndOfFile()`, `open()` og `close()` fra interfacet sekventiel tilgang.

```
file = open()
int i = 0;
while (!file.isEndOfFile())
    if (file.readNext() == search)
        return i;
    i++;
file.close()
return not found
```

40.2 Opskriv i pseudokode algoritmen for merge af to lister ved hjælp af operationerne `readNext()`, `isEndOfFile()`, `writeNext(data)`, `open()` og `close()` fra interfacet sekventiel tilgang.

```
file1 = open()
file2 = open()
i1 = file1.readNext()
i2 = file2.readNext()
merge = []
while (!file1.isEndOfFile() && !file2.isEndOfFile())
    if (i1 > i2)
        merge.push(i1)
        i1 = file1.readNext()
    else
        merge.push(i2)
        i2 = file2.readNext()
if (file1.isEndOfFile())
    while (!file1.isEndOfFile())
        merge.push(file1.readNext())
else
    while (!file2.isEndOfFile())
        merge.push(file2.readNext())
```

```
file1.close()  
file2.close()
```

40.3 I denne opgaver repræsenterer vi mængder som sorterede lister uden dubletter. For eksempel vil de to mængder $A = \{5, 3, 9, 8\}$ og $B = \{3, 2, 9, 10, 27\}$ være repræsenteret som disse sorterede lister:

$$A = [3, 5, 8, 9]$$

$$B = [2, 3, 9, 10, 27]$$

Beskriv en algoritme til at beregne repræsentationen af forenings mængden $X \cup Y$ ud fra repræsentationen af to mængder X og Y .

En algoritme ville foregå således.

Tag første element i begge lister, hvis de ikke er lig med hinanden tages den laveste. Hvis de er lig med hinanden tages kun én og den anden fjernes.

Dette udføres indtil en liste er tom hvorefter den anden ligges oven i.

40.4 **Beskriv en algoritme til at flette (merge) indholdet af tre sorterede lister A , B og C sammen til en sorteret liste D . Hvad er køretiden for din algoritme?**

Denne algoritme er den samme som mergesort. Dermed er køretiden $O(n)$

40.5 **Givet en algoritme til at flette indholdet af tre sorterede lister A , B og C sammen til én sorteret liste D (dvs. givet en løsning til opgave 4), beskriv en variant af Mergesort baseret på denne. Hvad er køretiden for din algoritme?**

For den første mergesort vil der være 2 lister med 1 element, som begge er sorteret

I denne mergesort vil det først element blive placeret først.

Ved denne næste merge vil det mindste element igen tages først og dermed vil det nye element placeres korrekt i listen.

40.6 Hvis en hashfunktion h er givet ved $h(x) = x \% 11$, på hvilke pladser i tabellen ender tallene **25, 75, 125, 175**?

25 \rightarrow 3
75 \rightarrow 9
125 \rightarrow 4
175 \rightarrow 10

40.7 Hvis en hashfunktion h er givet ved $h(x) = x \% 11$, hvor mange pladser i hashtabellen har mere end ét element, når der indsættes elementerne **34, 65, 122 og 155**?

34 \rightarrow 1
65 \rightarrow 10
122 \rightarrow 1
155 \rightarrow 1
Dermed 3 på 1

40.8 Beregn med lommeregner svaret på følgende: Hvis **3** elementer indsættes tilfældigt i et array med **7** pladser, hvad er sandsynligheden for, at der ikke er to elementer som ender på samme plads?

$$s_n = s_{n-1} \cdot \frac{7 - (n - 1)}{7}$$
$$s_0 = 1 \cdot \frac{7 - 0}{7} = 1$$
$$s_1 = 1 \cdot \frac{7 - 1}{7} = 0.86$$
$$s_2 = 0.86 \cdot \frac{7 - 2}{7} = 0.61$$
$$s_3 = 0.61 \cdot \frac{7 - 3}{7} = 0.35$$

- 40.9** Beregn med lommeregner følgende svaret på følgende:
Hvis 5 elementer indsættes tilfældigt i et array med 12 pladser, hvad er sandsynligheden for, at der ikke er to elementer som ender på samme plads?

$$\begin{aligned}s_0 &= 1 \\s_1 &= 1 \cdot \frac{12-1}{12} = 0.92 \\s_2 &= 0.92 \cdot \frac{10}{12} = 0.77 \\s_3 &= 0.77 \cdot \frac{9}{12} = 0.58 \\s_4 &= 0.58 \cdot \frac{8}{12} = 0.39 \\s_5 &= 0.39 \cdot \frac{7}{12} = 0.23\end{aligned}$$

- 40.1** Hvis en hashfunktion h er givet ved $h(x) = x \% 17$, på hvilke pladser i tabellen ender tallene **22, 72, 122, 172**?

$22 \rightarrow 5$
 $72 \rightarrow 4$
 $122 \rightarrow 3$
 $172 \rightarrow 2$

- 40.2** Hvis en hashfunktion h er givet ved $h(x) = x \% 17$, hvor mange pladser i hashtabellen har mere end ét element, når der indsættes elementerne **40, 74, 101 og 159**?

$40 \rightarrow 6$
 $74 \rightarrow 6$
 $101 \rightarrow 16$
 $159 \rightarrow 6$
Dermed 3 på plads 6

- 40.3** Lav et Java-program med input n og k der for situationen hvor n elementer indsættes tilfældigt i et array med k pladser finder sandsynligheden for, at der ikke er to elementer som ender på samme plads.

Kan findes i mappen collisionChance

- 40.4** Hvis 1000 elementer indsættes tilfældigt i et array med 1.000.000 pladser, hvad er sandsynligheden for, at der ikke er to elementer som ende på samme plads?

61% chance

- 40.5** Hvis n elementer indsættes tilfældigt i et array med 1.000.000 pladser, hvor stor skal n være for at sandsynligheden for, at der ikke er to elementer som ender på samme plads, bliver mindre end $\frac{1}{2}$

1177 fundet via programmet.

- 40.6** [Udfordrende] Beskriv en algoritme, der som input tager et tal K og to sorterede lister X og Y , hver med n tal, og finder ud af, om der findes et par af tal $x \in X$ og $y \in Y$ for hvilke $x + y = K$. Din algoritme skal køre i tid $O(n)$. Du skal argumentere for køretiden og for korrektheden af svaret.

```
additionElement(K,L1,L2):
int j = L2.length;
int i = 0;
while(i<L1.length && j >=0)
    if (L1[i]+L2[j]==K)
        return True;
    else if (L1[i]+L2[j]>K)
```

```

        j--;
    else
        i++;
return False;

```

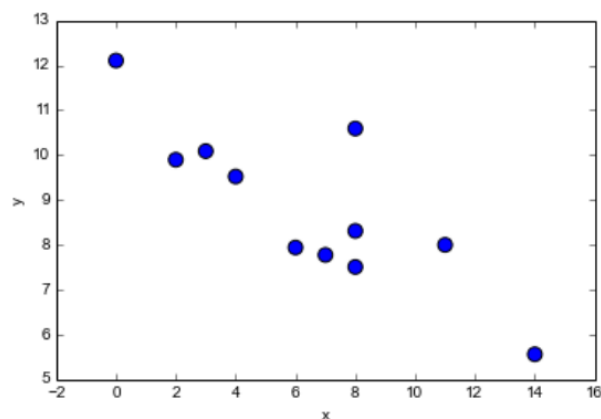
Med kun 1 loop vil den værste køretid være $O(n)$. Korrektheden kan findes i at, i tilfælde at additionen bliver for stor vil den rykke således at værdien vil blive mindre og bliver det større rykker den således listens værdier bliver mindre. Jeg tror dog at der er en fejl hvor det kan lade sig gøre at misse en værdi...

41 Uge

41.1 Exercise. k -Neares Neighbors: Prediction

What would the value of $x = 8$ be using 5-nearest neighbors and what form of learning is this exercise.

$$D = \begin{bmatrix} (8, & 8.31) \\ (14, & 5.56) \\ (0, & 12.1) \\ (6, & 7.94) \\ (3, & 10.09) \\ (2, & 9.89) \\ (4, & 9.52) \\ (7, & 7.77) \\ (8, & 7.51) \\ (11, & 8.0) \\ (8, & 10.59) \end{bmatrix}$$



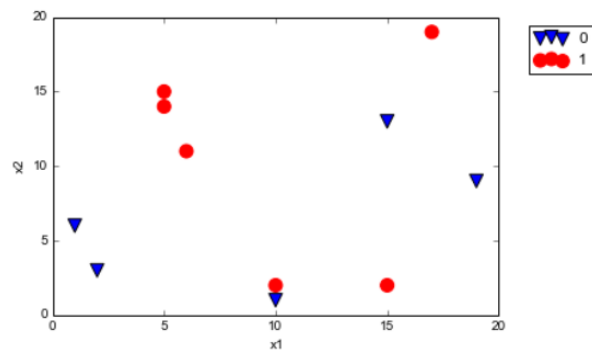
$$\hat{y}(x) = \frac{1}{k} \sum_{i|x_i \in N_k(x)} y_i = \frac{1}{5}(8.31 + 7.94 + 7.77 + 7.51 + 10.59) = 8.424$$

Supervised learning, regression. Supervised due to a correct value and regression due to the corresponding value being a value not being binary.

41.2 Exercise. k -Nearest Neighbors: Prediction

Predict $\vec{x} = (5, 10)$ with 5 nearest neighbors and determine the type of learning.

$$D = \begin{bmatrix} ((10, 2), 1) \\ ((15, 2), 1) \\ ((6, 11), 1) \\ ((2, 3), 0) \\ ((5, 15), 1) \\ ((5, 14), 1) \\ ((10, 1), 0) \\ ((1, 6), 0) \\ ((17, 19), 1) \\ ((15, 13), 0) \\ ((19, 9), 0) \end{bmatrix}$$



Here the difference was found and totalled between the two points and the best was chosen.

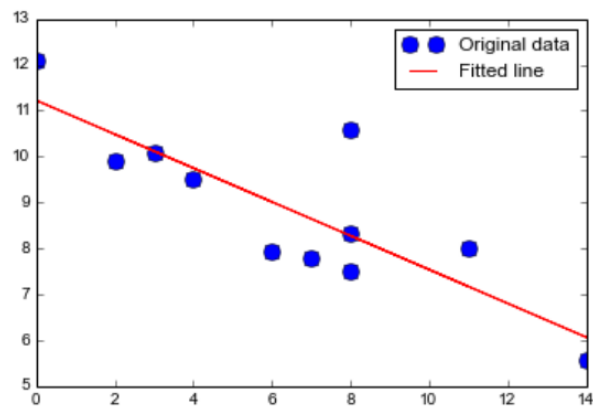
$$\frac{1+1+1+0+0}{5} = 1$$

Supervised learning classification.

41.3 Exercise. Linear Regression: Prediction

Find the value of $x = 8$ now with a linear regression model $g(x) = -0.37x + 11.2$

$$D = \begin{bmatrix} (8, 8.31) \\ (14, 5.56) \\ (0, 12.1) \\ (6, 7.94) \\ (3, 10.09) \\ (2, 9.89) \\ (4, 9.52) \\ (7, 7.77) \\ (8, 7.51) \\ (11, 8.0) \\ (8, 10.59) \end{bmatrix}$$



$$g(8) = -0.37 \cdot 8 + 11.2 = 8.24$$

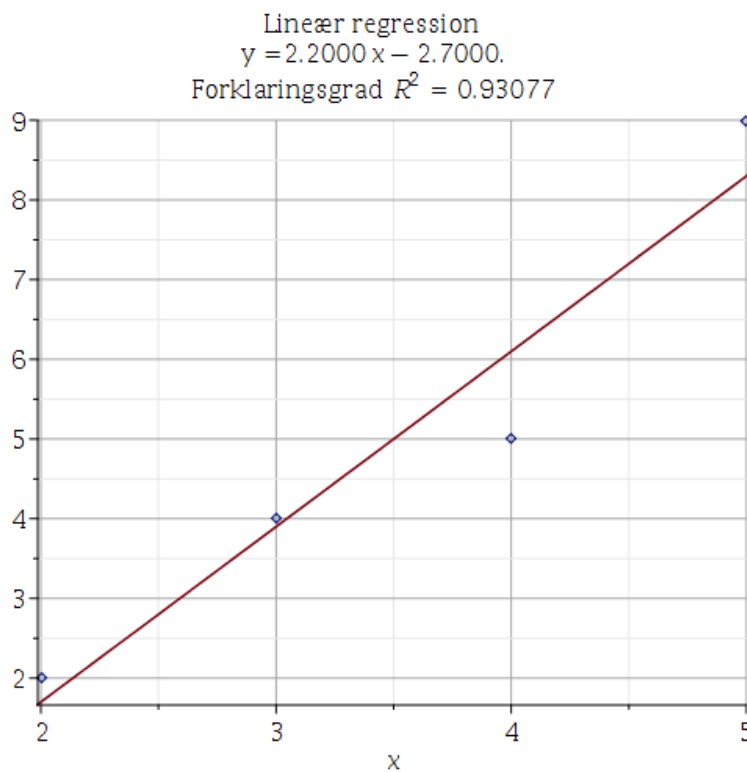
41.4 Exercise. Linear Regression: Training

Calculate the linear regression and the lost from the lose function.

```

dx := [2, 3, 4, 5]
dx := [2, 3, 4, 5]
dy := [2, 4, 5, 9]
dy := [2, 4, 5, 9]

```



```

f(x) := 2.2 x - 2.7
f := x ↦ 2.2 · x - 2.7

$$\sum_{i=1}^4 (dy[i] - f(dx[i]))^2$$

1.800000000

```

41.5 Exercise. Logical Functions and Perceptrons

Create truth table for the following perceptron gates

41.5.a OR gate

Here the $W_0 = 0.5, W_1 = 1, W_2 = 1$

$input_1$	$input_2$	sum	output
1	1	2	1
1	0	1	1
0	1	1	1
0	0	0	0

41.5.b NOT gate

Here the $W_0 = -0.5, W_1 = -1$

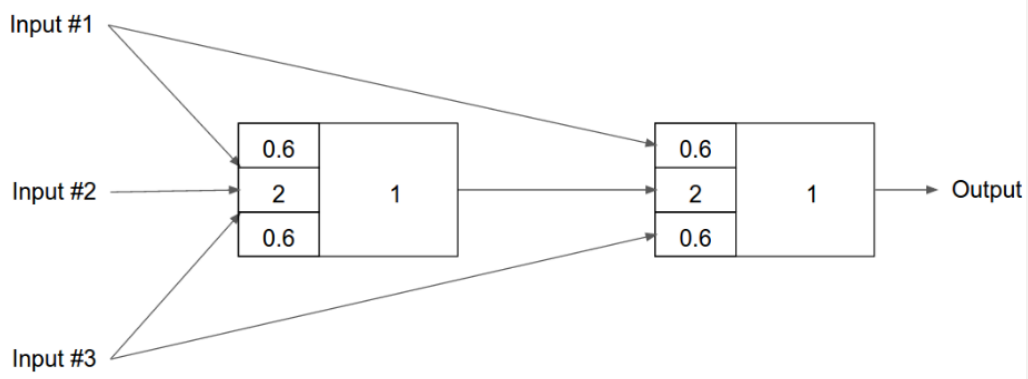
$input_1$	sum	output
1	-1	0
0	0	1

41.5.c Create NAND gate

$W_0 = -1.5, W_1 = -1, W_2 = -1$

41.6 Exercise. Multilayer Perceptrons

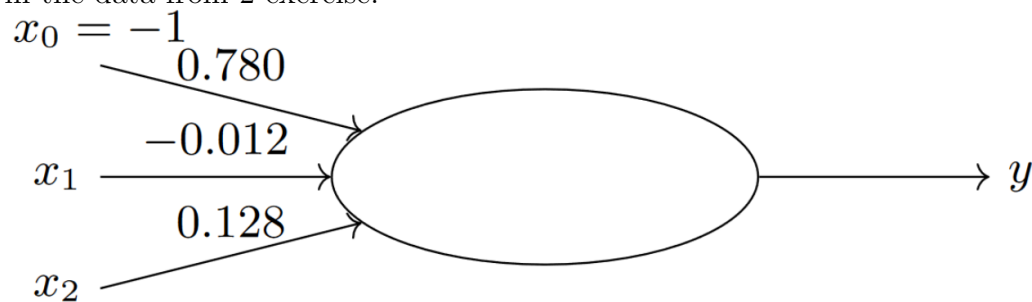
Determine the truth table for the following figure.



$input_1$	$input_2$	$input_3$	Perceptron1	Perceptron2
1	1	1	1	1
1	0	1	1	1
0	1	1	1	1
0	0	1	0	0
1	1	0	1	1
1	0	0	0	0
0	1	0	1	1
0	0	0	0	0

41.7 Exercise. Single Layer Neural Networks: Prediction

The following exercises is based on the following perceptron which was trained in the data from 2 exercise.



41.7.a Calculate output with $\vec{x} = (5, 10)$ using step function

$$-0.012 \cdot 5 + 0.128 \cdot 10 - 1 \cdot 0.78 = 0.440$$

Since the result is above zero it will return 1.

41.7.b Calculate output with $\vec{x} = (5, 10)$ using sigmoid function

$$\frac{1}{1+e^{-0.44}} = 0.6$$

The answer is above 0.5 therefore it returns 1

41.7.c Will the two functions always result in the same result, which one is more correct?

As it can be seen both function will result in the same result due to the sigmoid functions turning point being the at when the step function changes. As it can be seen the node is not perfect with 50% being correct

```

for i from 1 to 11 do  $-0.78 + 0.128 \cdot dx1[i] - 0.012 \cdot dx2[i]$  end do;
0.476
1.116
-0.144
-0.560
-0.320
-0.308
0.488
-0.724
1.168
0.984
1.544
for i from 1 to 11 do  $\frac{1}{1 + e^{-( -0.78 + 0.128 \cdot dx1[i] - 0.012 \cdot dx2[i] )}}$  end do;
0.6168028893
0.7532460037
0.4640620792
0.3635474598
0.4206757479
0.4236029911
0.6196351704
0.3265127646
0.7627833163
0.7279011823
0.8240454552

```

Figure 1: Beregning på punkter i D

41.7.d Make a plot with the predictions and find a line

41.8 Exercise. Expressivness of a single layer perceptron

A single layer perceptron will not be able to express a XOR gate

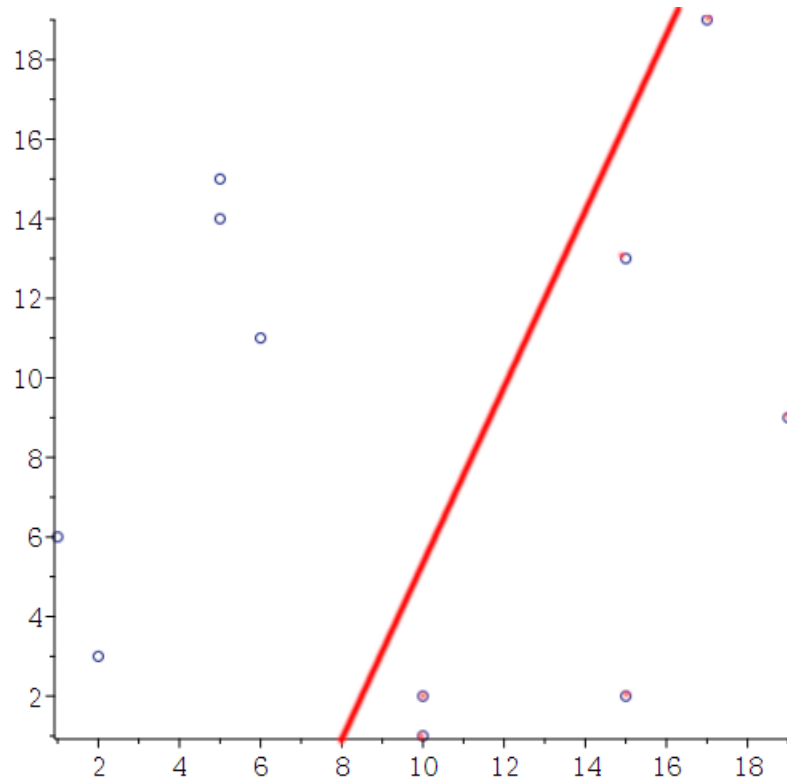
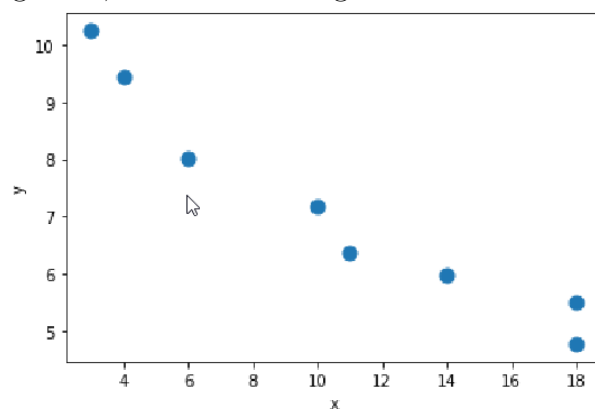


Figure 2: The ones classified is colores red

41.1 Exercise. k 'Nearest Neighbors: Prediction

Find $x = 12$ using 3 nearest neighbors, on the following data.

$$D = \begin{bmatrix} 11. & 6.36 \\ 14. & 5.98 \\ 6. & 8.02 \\ 10. & 7.17 \\ 18. & 5.51 \\ 18. & 4.77 \\ 3. & 10.25 \\ 4. & 9.45 \end{bmatrix}$$



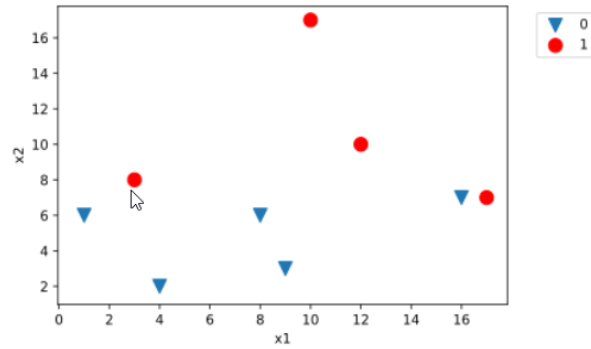
$$\frac{7.17+6.36+5.98}{3} = 6.50$$

This is a supervised learning regression.

41.2 Exercise. k -Nearest Neighbors: Prediction

Find $\vec{x} = (14, 8)$ using 3 nearest neighbors, on the following data.

$$D = \begin{bmatrix} ((4, 2), 0) \\ ((16, 7), 0) \\ ((10, 17), 1) \\ ((12, 10), 1) \\ ((8, 6), 0) \\ ((3, 8), 1) \\ ((1, 6), 0) \\ ((9, 3), 0) \\ ((17, 7), 1) \end{bmatrix}$$

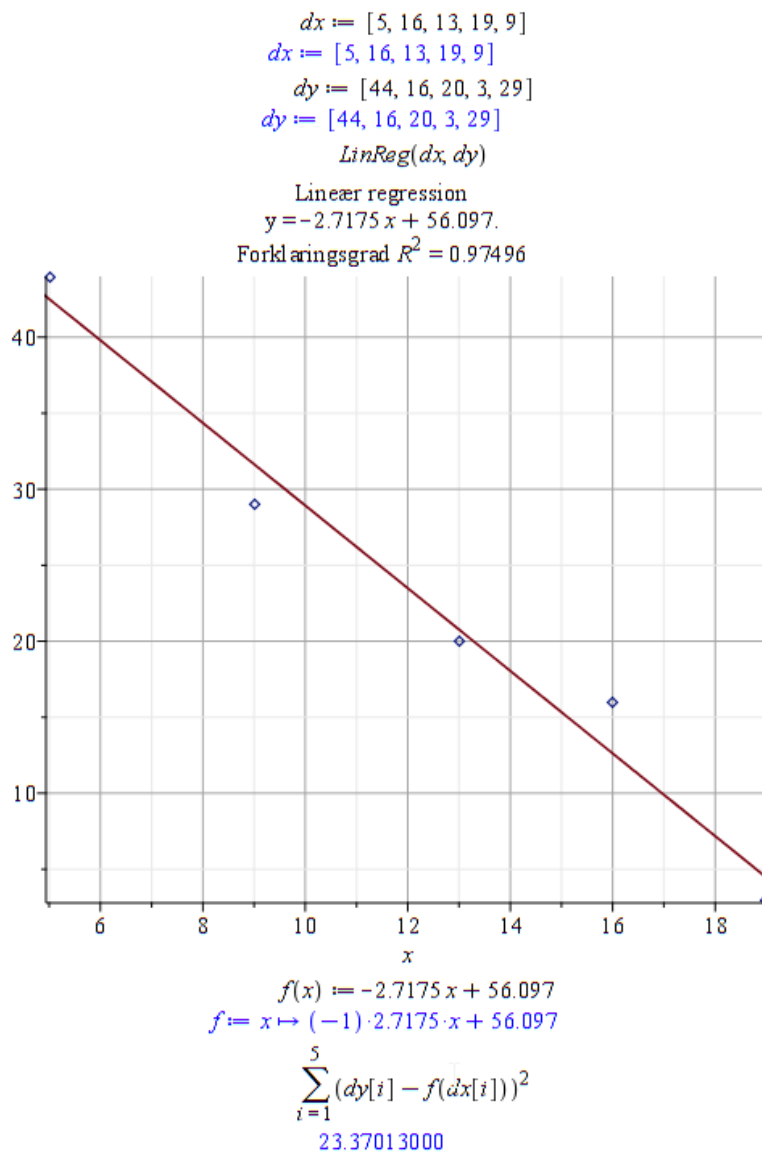


$1 + 0 + 1 = 2$ output 1
Supervisedclassification

41.3 Exercise. Linear Regression: Training

Calculate the linear regression and the lost.

$$D = \begin{bmatrix} 5 & 44 \\ 16 & 16 \\ 13 & 20 \\ 19 & 3 \\ 9 & 29 \end{bmatrix}$$



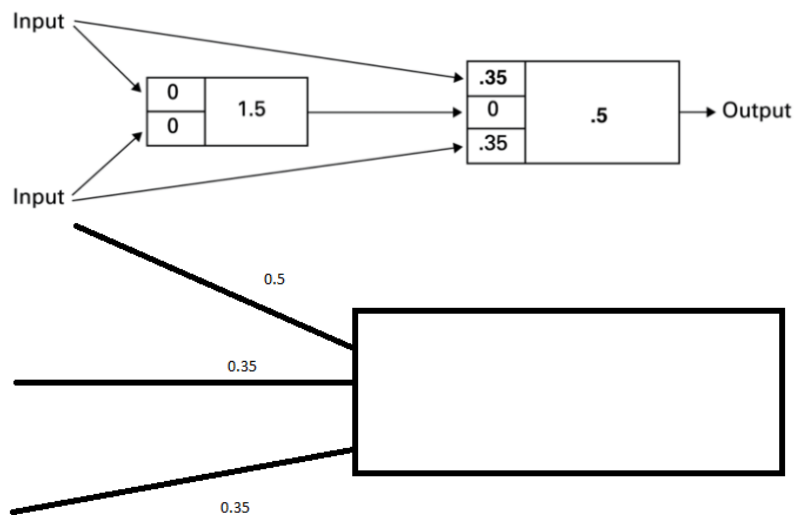
41.4 Exercise. Feed-Forward Neural Network: Single Layer Perceptron

Determine the parameters of a single perceptron (that is, a neuron with step function) that implements the majority function: for n binary inputs the function outputs a 1 only if more than half of its inputs are 1.

It will simply be a weight of 1 except the bias $w_0 = \lfloor n \rfloor$

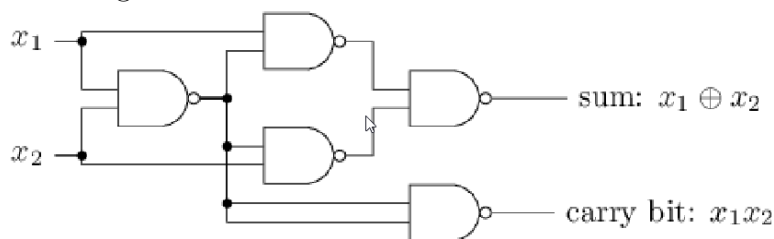
41.5 Exercise. Single Layer Perceptrons

Make the following neural network into a perceptron.



41.6 Exercis. Logical Functions and Neural Networks

We have to convert the following circuit with perceptrons from exercis 5. Just imagine it.



43 uge

43.1 Beregn følgende

43.1.a L_3 -normen af $\vec{v} = (-2, 5)$.

$$(-2.5^3 + 5^3)^{1/3} = 4.78$$

43.1.b L_7 -normen af $\vec{v} = (4.5, -3.2)$.

$$(4.5^7 - 3.2^7)^{1/7} = 4.38$$

43.1.c L_1 -normen af $\vec{v} = (5, 9)$.

$$(5^1 + 9^1)^{1/1} = 14$$

43.1.d $L_{1.5}$ -normen af $\vec{v} = (2, 3)$.

$$(2^{1.5} + 3^{1.5})^{1/1.5} = 4.01$$

43.1.e L_∞ -normen af $\vec{v} = (4.5, -3.2)$.

$$(4.5^\infty - 3.2^\infty)^{1/\infty} = \max(4.5, -3.2) = 4.5$$

43.2 For $\vec{p} = (1, 2, 3)$ og $\vec{q} = (0, 5, -2)$ beregn følgende:

43.2.a Afstanden $\text{dist}_2(\vec{p}, \vec{q})$.

$$(|1 - 0|^2 + |2 - 5|^2 + |3 + 2|^2)^{1/2} = 5.92$$

43.2.b Afstanden $\text{dist}_3(\vec{p}, \vec{q})$.

$$(|1 - 0|^3 + |2 - 5|^3 + |3 + 2|^3)^{1/3} = 5.35$$

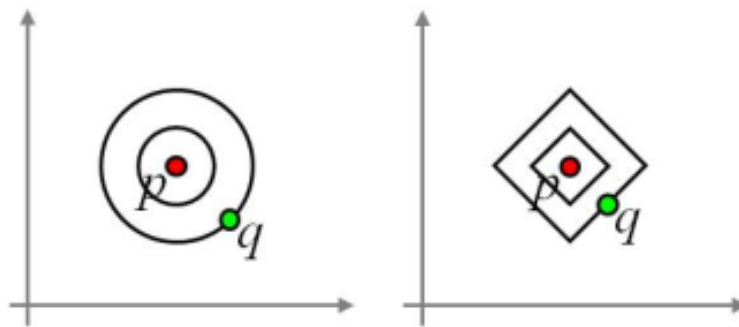
43.2.c Afstanden $\text{dist}_1(\vec{p}, \vec{q})$.

$$(|1 - 0|^2 + |2 - 5|^2 + |3 + 2|^2)^{1/2} = 35$$

43.2.d Afstanden $\text{dist}_\infty(\vec{p}, \vec{q})$.

$$(|1 - 0|^\infty + |2 - 5|^\infty + |3 + 2|^\infty)^{1/\infty} = \max(1, 3, 5) = 5$$

43.3 Forklar figuren mudt på side 18 i Melih Kandemirs slides. Dvs. forklaar hvorfor mængden af alle punkter \vec{q} i en given afstand r fra et punkt \vec{q} (også kaldet "cirklen" om \vec{q} med radius r) har en sådan facon, når afstanden er givet ved dis_1 .



Det kommer af at formen er ens med definitionen af en cirkel nemlig $(x - x_c)^2 + (y - y_c)^2 = r^2$ hvor det ene punkt er centrum for cirklen.

43.3 Forklar også figuren til højre på samme side

En måde at se det på er, at afstanden vil her være hypotenusen i en retvinklet trekant. Dermed ved vinklerne bliver 0, 90, 270 og 360, vil de to kateter blot blive summeret og de andre steder vil det være hypotenusen som er afstanden.

43.3 Forsøg også at forklare, hvorfor L_∞ er et godt navn for max-normen, når man sammenligner med definitionen af L_p

Da potensen og kvadratroden er så stor vil det betyde at desto højere tallet er vil det have markant mere effekt og derfor tages blot det højeste tal.

43.4 Consider the five pictures given in Figure 1 each with 36 pixels.

43.4.a Extract from each picture a color histogram with the bins *red*, *orange*, and *blue* (the white pixels are ignored)

- a - 1 4 4

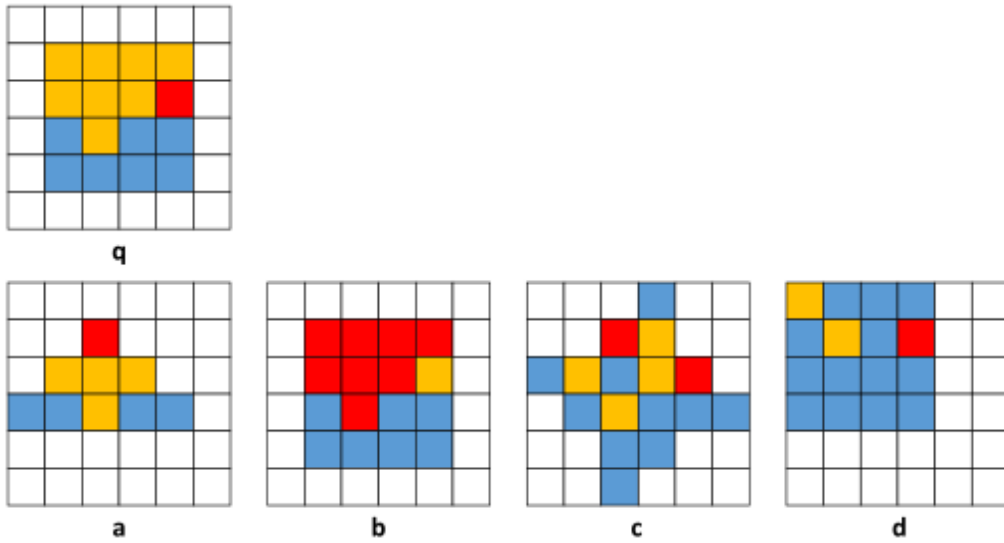


Figure 3: 6×6 pixel pictures

- b - 8 1 7
- c - 2 4 10
- d - 1 2 13
- q - 1 8 7

43.4.b For each of the pictures a to d , calculate their similarity to q using Euclidean distance (i.e. using dist_2)

- a - $(|1 - 1|^2 + |4 - 8|^2 + |4 - 7|^2)^{0.5} = 5$
- b - $(|8 - 1|^2 + |1 - 8|^2 + |7 - 7|^2)^{0.5} = 9.9$
- c - $(|2 - 1|^2 + |4 - 8|^2 + |10 - 7|^2)^{0.5} = 5.1$
- d - $(|1 - 1|^2 + |2 - 8|^2 + |13 - 7|^2)^{0.5} = 8.49$

Therefore the closes approximation to q is a

43.5 Repetér definitionen af en centroide for en cluster C bestående af følgende tre punkter

$$C = \{(2, 3), (5, 5), (4, 1)\} \left(\frac{2+5+4}{3}, \frac{3+5+1}{3} \right) = (3.67, 3)$$

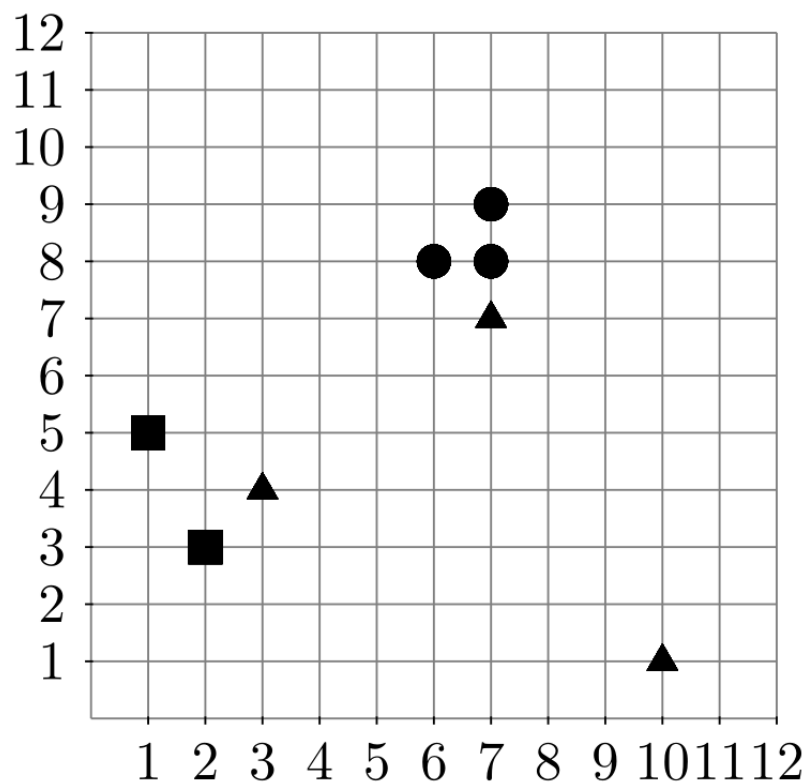
43.6 Check beregningen af de to centroder i figuren på side 32

blue $\{(1, 5), (3, 4), (10, 1)\}$

red $\{(7, 7), (7, 8), (6, 8), (7, 9)\}$ red centroid $\left(\frac{1+3+10}{3}, \frac{5+4+1}{3} \right) = (4.67, 3.33)$

blue $\left(\frac{7+7+6+7}{4}, \frac{7+8+8+9}{4} \right) = (6.75, 8)$

43.7 Consider the following data set (with 8 objects in \mathbb{R}^2) used in the lecture:



43.7.a Compute a complete partitioning with $k = 2, 3, 4, 5$ using k means method

$k = 2$: (7.4,6.6), (2,4) - TD2 = 54.4

$k = 3$: (10,1),(6.75,8),(2,4) - TD2 = 6.75

$k = 4$: (10,1),(2.5,3.5),(1,5),(6.75,8) - TD2 = 3.75

$k = 5$: (10,1),(6.5,7.5),(1.5,4),(3,4),(7,8.5) - TD2 = 4

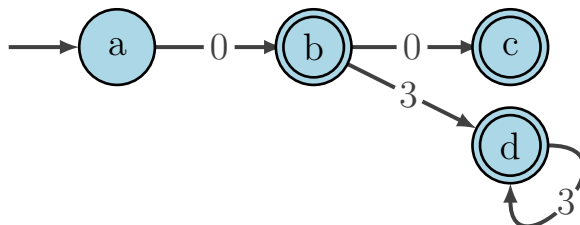
When the number of clusters became larger, many times it would cluster to a lower amount and clusters would just be at (0,0).

43.8 Repeter forskellen på Forgy-Lloyd og MacQueen udgaverne af k-means algoritmen, giver de to udgaver altid samme resultat.

Nej, ud fra punkternes tilfældige placering, giver det en variation ved begge algoritmer og dermed vil de aldrig med garanti give ens resultater. Derudover kan algoritmen også udføres på samme punkter og også give forskellige løsninger

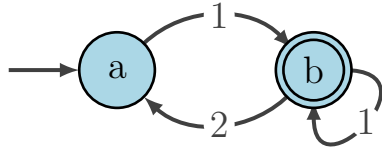
44 Uge

44.1 Exercise



The following DFA will accept string starting with 0 followed by infite 3 or a zero or nothing.

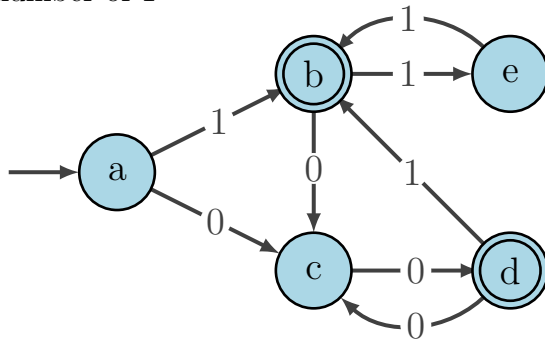
44.2 Exercise



The following DFA will accept string startign with 1 followed by either any number of 1 or a 2 followed by any number of 1.

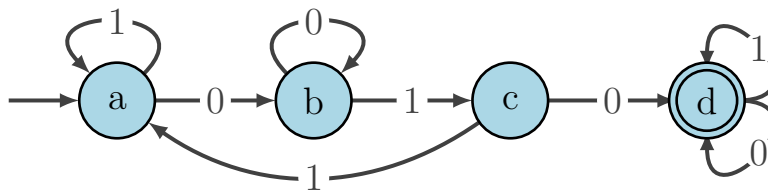
44.3 Exercis

Write a DFA which accepts strings containing a even number of zeros and odd number of 1



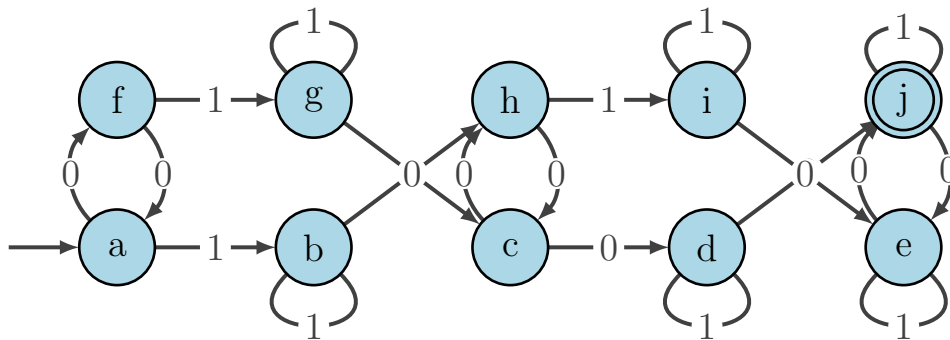
44.4 Exercise

Make a DFA that accepts a string of 0 and 1 which contains 010



44.5 Exercise

Define a DFA that recognises the following languageL Akk strings of 0s and 1s that contain at least two occurrences of 10 and an even number of 0s.



44.6 Exercise

What is the language of the following CFG?

$$S \rightarrow ab$$

$$S \rightarrow SS$$

Its the language consisting of any amount of ab

44.7 Exercise

Write two different ways of 000111 using:

$$S \rightarrow 0M1$$

$$M \rightarrow M1$$

$$M \rightarrow 0M$$

$$M \rightarrow 0$$

$$M \rightarrow 1$$

$SMMMM$ and $MMMMMM$

44.8 Exercise

What is the language of the following CFG?

$$S \rightarrow 0MM1$$

$$M \rightarrow M1$$

$$M \rightarrow 0M$$

$$M \rightarrow 0$$

$$M \rightarrow 1$$

The string of 0 and 1 which starts with any amount of zeros and end with any amount of 1.

44.9 Exercise

Write a CGF which accepts input with any number of 0 and any amount of 1 after

$$S \rightarrow 0S1$$

$$S \rightarrow 01$$

44.10 Exercise

Write a DFA of the following CFG

$$S \rightarrow 0M$$

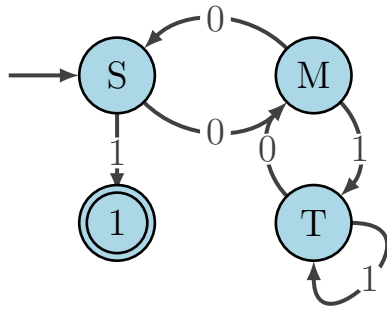
$$S \rightarrow 1$$

$$M \rightarrow 0S$$

$$M \rightarrow 1T$$

$$T \rightarrow 0M$$

$$T \rightarrow 1T$$



44.11 Exercise

Write a CFG which describes the parenthesis and addition language

$$\begin{aligned}
 S &\rightarrow \text{number} : \\
 S &\rightarrow \text{number} : S \\
 S &\rightarrow +S \\
 S &\rightarrow (S)
 \end{aligned}$$

45 uge

45.1 Prove that the best online algorithm for the ski problem has a competitive ratio on $\frac{19}{10}$

The ski costed 1 unit to rent a day and 10 to buy.

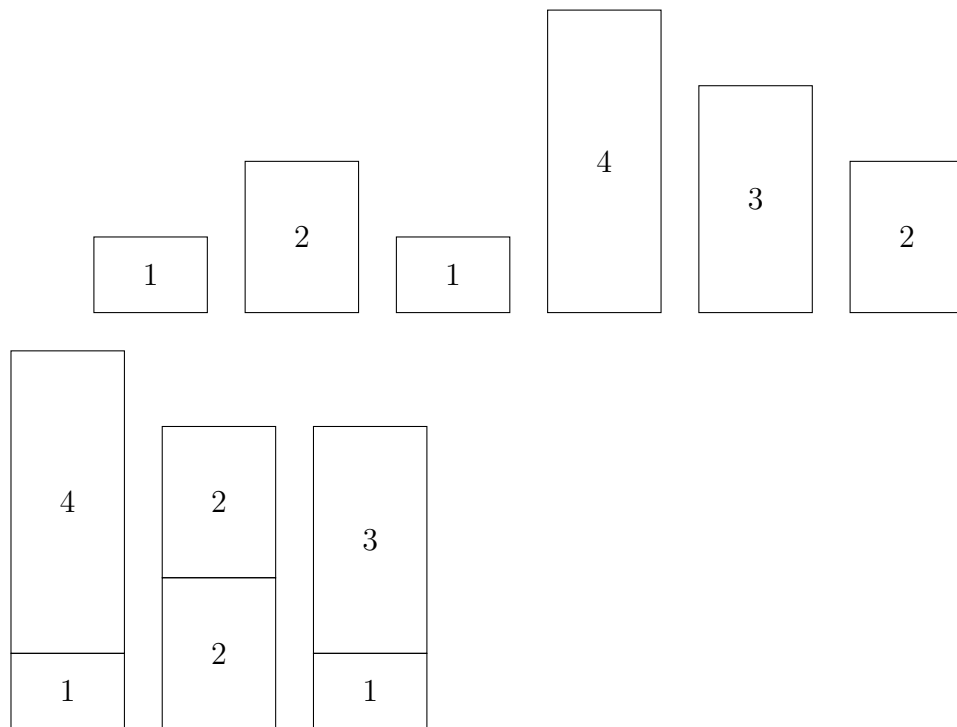
The online algorithm suggested on buying day 9, which results in a competitive ratio on $\frac{19}{10}$

The alternative is buy on day 5 and day 15

Buy on day 5 worst case scenario is return on day five which cost 14 for the online algorithm and 5 if only renting which is a competitive ratio on $\frac{14}{5}$

Buy on day 15 will cost 24 at worst case and the offline will buy on day 1 which will be 10 therefore the competitive ratio is $\frac{24}{10}$

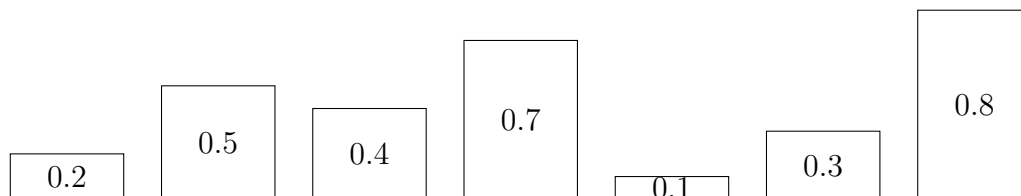
45.2 For the scheduele algorithm, what are the result of $m = 3$

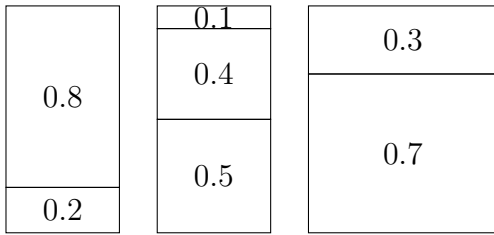


45.3 Make input for any algorithm with $m = 2$ which will result in better result than $\frac{3}{2}$ of the optimum

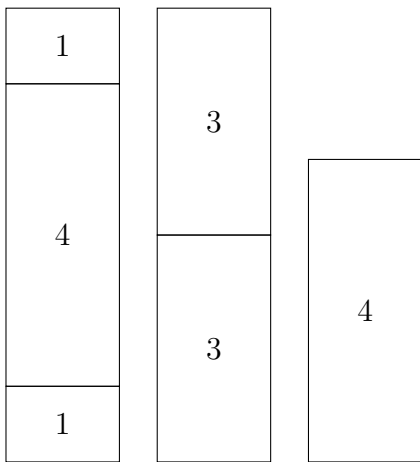
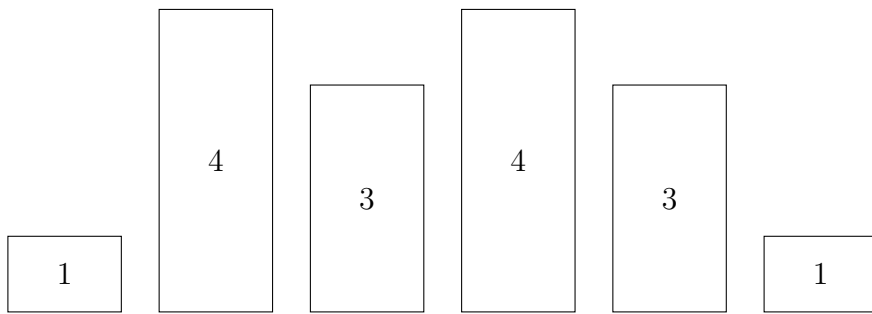
From the data 0.3 0.3, if the algorithm stacks 0.3 0.3 we give it the 0.1 input. If it does not stack we give it a 6.

45.4 Show that the following data can be in three bins

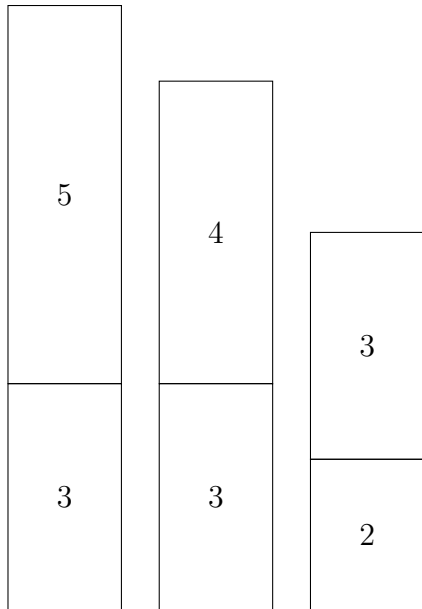




45.5 Use First Fit on the following data, where the max size is 6



45.6 Why can the following result not be amde by First Fit, max size is 9



Because the 2 in the last row would be able to be put on bin 2 and therefore the last bin should only be 3.

45.1 Find a squence where Ff performs $\frac{5}{3}$ times worse than OPT

$$37 \cdot (\frac{1}{43} + \frac{1}{10000}), 11 \cdot (\frac{1}{7} + \frac{1}{10000}), 12 \cdot (\frac{1}{3} + \frac{1}{10000}), 14 \cdot (\frac{1}{2} + \frac{1}{10000})$$

This will result in bin 1 being filled with $\frac{1}{43}$, then 2 bins with $\frac{1}{7}$, then 6 bins with 2 thirds and 13 bins with a half. In total 22

For OPT it will make 11 bins with 1 half, 1 third, $\frac{1}{7}$ and $\frac{1}{43}$ and two bins with the rest. Therefore the result is $\frac{22}{13}$

46 Uge

46.1 Which of the following formulas are satisfiable

46.1.a $A \wedge B$

Satisfiable if A and B are true

46.1.b $A \vee B$

Satisfiable if A or B are true

46.1.c $A \rightarrow B$

Satisfiable if A and B are true

46.1.d $A \wedge \neg A$

Not satisfiable

46.1.e $A \vee \neg A$

Satisfiable always true

46.2 Which if the following formulas are equivalent
(same assignment satisfy)

1. $\neg A \wedge B$

2. $\neg A \vee B$

3. $A \rightarrow B$

4. $(A \rightarrow B) \wedge (\neg B \rightarrow A)$

5. $(\neg A \rightarrow B) \wedge (\neg B \rightarrow \neg A)$

For these the same assignment will return true

$1=2=3=5$

$4=2=3=5$

But 2 and 3 are equivalent and 4 and 5 are equivalent

46.3 Convert the following formulas into CNF

46.3.a $\neg A \wedge B$

46.3.b $\neg A \vee B$

46.3.c $A \rightarrow B$

$\neg A \vee B$

46.3.d $(A \rightarrow B) \wedge (\neg B \rightarrow A)$

$(\neg A \vee B) \wedge (B \vee A)$

46.4 Breaking symmetry in N-Towers and N-Queens

46.4.a Write two clauses that forbid solutions where there is a queen in the right half of the first row

$$(\neg X_{1,1}) \wedge (\neg X_{1,2})$$

46.4.b Instead of adding two clauses change an existing clause

$(X_{1,1} \vee X_{1,2} \vee X_{1,3} \vee X_{1,4})$ to $(X_{1,3} \vee X_{1,4})$ This will determine that it must be either one of those two.

46.6 The formula from Slide 11 contains redundant information. For Example $X_{1,1} \rightarrow \neg X_{1,2}$ and $X_{1,2} \rightarrow \neg X_{1,1}$ are equivalent. Understand and remove these redundancies:

46.6.a Why do these redundancies occur?

They are often not directly identifiable since to construct a boolean formula it is often taken from one end to another.

46.6.b Identify all such redundancies!

$$X_{1,1} \rightarrow \neg X_{1,2} \equiv X_{1,2} \rightarrow \neg X_{1,1}$$

$$X_{1,1} \rightarrow \neg X_{2,1} \equiv X_{2,1} \rightarrow \neg X_{1,1}$$

$$X_{1,2} \rightarrow \neg X_{2,2} \equiv X_{2,2} \rightarrow \neg X_{1,2}$$

$$X_{2,1} \rightarrow \neg X_{2,2} \equiv X_{2,2} \rightarrow \neg X_{2,1}$$

46.6.c Write down a simplified formula without redundancies

It the right row of the previous align plus $X_{1,1} \vee X_{1,2} \wedge X_{2,1} \vee X_{2,2}$

46.6.d Convert the formula to CNF

$$[[\neg X_{1,1} \neg X_{1,2}], [\neg X_{1,1}, \neg X_{2,1}], [\neg X_{1,2}, \neg X_{2,2}], [\neg X_{2,1}, \neg X_{2,2}], [X_{1,1}, X_{1,2}], [X_{2,1}, X_{2,2}]]$$

46.6.e Write the formula in DIMACS format

```
p cnf 4 6
-1 -2 0
-1 -3 0
```

-2 -4 0
-3 -4 0
1 2 0
3 4 0

46.6.f Run it in a SAT and test result

Result - $v1 = 2 = 340$

It here came up with a result with the tower in upper left and lower right

46.1 Which of the following formulas are satisfiable

46.1.a $(A \rightarrow B) \wedge (B \rightarrow A)$

A and B true

46.1.b $(A \rightarrow B) \wedge (B \rightarrow A) \wedge A$

A and B true

46.1.c $(A \rightarrow B) \wedge (B \rightarrow A) \wedge \neg A$

A and B false

46.1.d $(A \rightarrow B) \wedge (B \rightarrow A) \wedge (\neg A \rightarrow \neg B) \wedge (\neg B \rightarrow A)$

A and B true

46.2 Which of the following formulas are equivalent

- $(A \rightarrow B) \wedge (\neg B \rightarrow A)$
- $(A \rightarrow \neg B) \wedge B \rightarrow A)$
- $(\neg A \vee \neg B) \wedge (A \vee \neg B)$
- $(B \vee A) \wedge (\neg A \vee B)$

A and B true

1,4

A true, B false

2,3

46.3 Convert to CNF

46.3.a $(\neg A \rightarrow B) \wedge (\neg B \rightarrow \neg A)$

$$(A \vee B) \wedge (B \vee \neg A)$$

46.3.b $A \rightarrow (\neg(B \wedge D))$

$$\neg A \vee \neg B \vee \neg D$$

46.3.c $A \rightarrow (\neg(B \vee D))$

$$\neg A \vee (\neg B \wedge \neg D)$$

46.3.d $A \rightarrow (\neg(B \rightarrow (C \wedge D)))$

$$\neg A \vee B \wedge \neg C \vee \neg D$$

47 47

47.1 Given the following relation schema:

Band(*name* : CHAR(20), *formed_in* : INTEGER)

Which of the following are valid tuples of the Band relation?

- ('Foo Fighters', 1994)
- (1991, 'Incubus')
- ('Massive Attack')
- ('Disturbed', '1996')

Band	formed_in
Foo fighters	1994

47.2 The relation schema of task 1 together with the vald tuples define a relation instance. Visualize this relation instance as a table

47.3 Given the following relation instance

Movies				
mid	title	director	production_year	budget_usd
0	'Matrix'	'The Wachowskis'	1999	63000000
1	'Raiders of the Lost Ark'	'Steven Spielberg'	1981	20000000
2	'The Shawshank Redemption'	'Frank Darabont'	1994	25000000
3	'Twilight'	'Robert Benton'	1998	20000000
4	'Dead Poets Society'	'Peter Weir'	1989	16400000
5	'Django Unchained'	'Quentin Tarantino'	2012	100000000
6	'Pulp Fiction'	'Quentin Tarantino'	1994	8500000
7	'Twilight'	'Catherine Hardwicke'	2008	37000000

Figure 4

Which of the following atributes sets are possible primary keys (i.e., the data instance above is consistent with choosing that set of attributes as the primary key)?

- mid
- title
- director
- title, director
- director, production_year

1, 4, 5

47.4 Given the following Entity-Relationship diagram

How could this ER diagram be modeled in the relational model? Provide the relation schemas. What would change if the relationship "develops" had an attribute "start date"? Note that here is no desingation of keys for entities. It is part of the task to consider what is a good choice of keys (this is a data modeling choice, for which there is no single "right answer")
 GAME('name':char(20),'Release date': char(10), 'Budget': integer)

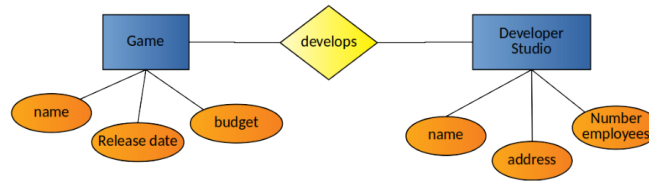


Figure 5

Developer Studio('name': char(20),'Address':char(40),'Number employees':integer)
 develops('name':char(20),'address': char(40))

47.5 You are given the relation instance defined in task 3

How many tuples do the relations resulting from the following relational operations contain? [Recall that in the relational mode, relations are sets, so there can be no duplicates among (entire) tuples/rows.]

- $\sigma_{production_year > 1994}(Movies)$ - 4
- $\pi_{mid, title, director}(Movies)$ - 8
- $\pi_{director}(Movies)$ - 7

47.6 You are given the following ER-diagram:

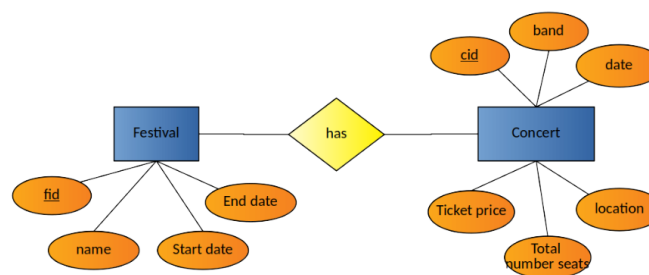


Figure 6

and the corresponding relations:

- Concert(cid: integer, band: char(20), date char(20), location: char(20), total_number_seats: integer, ticket_price: float)

- Festival(fid integer, name: char(20), start_date: char(20), end_date: char(20))
- FestivalHasConcert(festival: integer, concert: integer)

Here, underlined attributes are primary keys of the relation and dashed underlined attributes are foreign keys. Specify the SQL command that creates the table corresponding to the Concert relation of task. Also specify the SQL command that creates a corresponding table for the FestivalHasConcert relation. [Recall that FestivalHasConcert's festival and concert attributes are foreign keys referencing the fid in the festival and cid in the concert relation]

```
CREATE table Concert(cid: integer, band: char(20), date: char(20), location: char(20), total_number_sears: integer, ticker_price: float, Primary Key (cid))
CREATE table FestivalHasConcert(festival: integer foreign key reference Concert(cid), concert integer foreign key reference Festival(fid))
May also be FOREIGN KEY (concert) REFERENCES Concert
```

47.7 Specify an SQL command that deletes from the Moveis table all moeis that were not produced in 1994

```
DELETE FROM Moveis WHERE production_year != 1994;
```

47.8 You want to retriive the titles f all moveis from the Moviestable of task3 that were produced in 1994 and directed by Quentin Tarantino. Express the query in bth theese ways:

- As an expression in relational algebra
- As an SQL command

$\pi_{title} \sigma_{prouction_year=1994 \wedge director="QuentinTarantino"}(Movies)$
 Select title From Movies where production_year == 1994 and director == "Quentin Tarantino"

47.9 Consider the Movies table of task 3. Provide in SQL one INSERT and one DELETE command that can be executed to change it into the following table

Movies				
mid	title	director	production_year	budget_usd
0	'Matrix'	'The Wachowskis'	1999	63000000
1	'Raiders of the Lost Ark'	'Steven Spielberg'	1981	20000000
5	'Django Unchained'	'Quentin Tarantino'	2012	100000000
7	'Twilight'	'Catherine Hardwicke'	2008	37000000
8	'The Lord of the Rings'	'Peter Jackson'	2001	93000000

Figure 7

DELETE FROM Movies WHERE production_year < 1995 and production_year > 1988
 INSERT INTO Movies (9,'The Lord of the Rings', 'Peter Jackson', 2001, 93000000)

47.10 Specify an SQL command without set operations (UNION or EXCEPT) that retrieves all movies from the Movie table, that have been produced before 1990 or that have a budget of at least 30 million USD. State the same query as a relational algebra expression

SELECT * FROM Movies WHERE production_year < 1990 or 30000000 < budget_usd

$\sigma_{production_year < 1990 \vee 30000000 < budget_usd}(Movies)$

47.11 Solve task 10 with SQL operations (UNION OR EXCEPT). State the same query as a relational algebra expression.

SELECT * FROM Movies WHERE production_year < 1990 EXCEPT SELECT * FROM Movies Where budget_usd > 30000000

$\sigma_{production_year < 1990} - \sigma_{budget > 30000000}$

47.12 Specify an SQL command without set operations (UNION or EXCEPT) that retrieves all movies from the Movie table if task 3 that either

- have been produced before 1990 with a budget of at least 30 million USD
- or have been produced after 2010

```
SELECT * FROM Movies WHERE production_year < 1990 and budget_usd > 30000000 or 2010 < production_year
```

47.13 Specify an SQL command that retrieves all pairs of movies from the Movies table for task 3 that have been directed by the same director.

For instance if two movies 'movie1' and 'movie2' were directed by the same director, the result relation should, amongst others, contain the following tuples:

- (movie1, movie2)
- (movie2, movie1)

```
SELECT title FROM Movies WHERE director = dir CROSS JOIN SELECT title FROM Movies WHERE director = c
```

ALTERNATIVE

```
SELECT * FROM Movies M1, Movies M2 WHERE M1.director = M2.director AND M1.mid != M2.mid
```

47.14 Specify an SQL command that retrieves all pairs of movies (movie1, movie2) from the Movies table for task 3 with movie1's budget exceeding the budget of movie2

For instance if a movie 'movie5' has a larger budget than 'movie8', the result relation should contain, amongst others the following tuple: (movie5, movie8)
State the same query as an relational algebra expression

SELECT title FROM Movies WHERE budget <= bud CROSS JOIN SELECT title FROM Movies WHERE budget < bud
 Alt. SELECT * FROM Movies M1, Movies M2 WHERE M1.budget_usd > M2.budget_usd;

47.1 Which of the following statements are true?

- ✓ The result of applying a relational algebra operator to a relation instance is another relation instance
- Entities of the ER-diagram can not be described by relations in the data model.
- A relation instance needs to contain at least one tuple
- Integrity constraints are specified when querying the database
- ✓ Primary keys and foreign keys are types of integrity constraints
- The relational selection operator always returns a relation instance with fewer tuples.
- ✓ The relational projection operator may return a relation instance with fewer tuples.
- The SQL UNION operator can be applied to two relation instances if they have the same number of attributes

47.2 Joins are compound operator which we did not cover in the lecture. They are useful for joining (combining) the data contained in multiple relations together. In relational algebra the conditional join operator \bowtie_C (also called the θ -join operator) is defined by

$$R1 \bowtie R2 = \sigma_C(R1 \times R2)$$

In words: A conditional join can be calculated by first computing the cross product of the two relations $R1$ and $R2$ followed by a selection using the condition C .

We now look at the following conditional join on relations from task 6.

$\text{Festival} \bowtie_{fid=festival} \text{FestivalHasConcert}$

This join combines the two relations Festival and FestivalHasConcert using the attribute fid of the Festival relation, and the festival attribute of the FestivalHasConcert relation. Specifically it combines those tuples of the two relations for which the equality condition holds.

What is the relation schema of the result relation?

It returns a tuples with the festival and concert id if the concert is at the festival.

47.3 Specify an SQL command that calculates hte conditional join given in task 2

SELECT name, cid FROM Festival, FestivalHasConcert WHERE Festival.fid = FestivalHasConcert.fid

47.4 Specify an SQL command that calculates the following nested relational operation involving two conditional joins

Festival ⋈_{fid=festival} FestivalHasConcert ⋈_{concert=cid} Concert

SELECT cid, fid FROM Festival, FestivalHasConcert, Concert WHERE Festival.fid = FestivalHasConcert.fid and FestivalHasConcert.cid = Concert.cid;

48 Uge

The following answers a gathered through the RSA program.

48.1 Suppose in RSA the public key is $PK = (1517, 13)$. Which of the following is the RSA encryption if the message 43

$$E(m, PK) = 894 \bmod 1517$$

$$43^{13} \bmod 1517 = 894 \bmod 1517$$

48.2 Is one of the following the multiplicative inverse if 49 modulo 221

212

48.3 Which of the following sets of public key (OK) and secret key (SK) is a valid set of RSA keys (ignoring the numbers are not large enough)

48.3.a $PK = (91, 37); SK = (91, 23)$

$$91 = 7 \cdot 13$$

$$37 \cdot 23 \equiv 1 \pmod{(7-1) \cdot (13-1)}$$

$$851 \equiv 1 \pmod{72}$$

$$851 \equiv 59 \pmod{72}$$

Not a working pair

48.3.b $PK = (143, 77); SK = (143, 53)$

$$143 = 11 \cdot 13$$

$$77 \cdot 53 \equiv 1 \pmod{(11-1) \cdot (13-1)} \quad 4081 \equiv 1 \pmod{120}$$

This works!

48.3.c $PK = (231, 59); SK = (231, 47)$

231 has a prime factorization of 3, 7 and 11 and therefore not a valid number

48.3.d $PK = (107, 25); SK = (107, 30)$

107 is a prime and therefore not valid

48.4 In the Sieve of Eratosthenes, how many lists have been created at the point where the number 13 is the first element in the list?

The first elements will be:

2, 3, 5, 7, 11, 13 Therefore 6

48.5 Consider an RSA system with Alice public key $n = 1517$ and $e = 17$. Note that $1517 = 37 \cdot 41$.

48.5.a Find Alice's secret key d . Use the extended Euclidean Algorithm from page 42 of the slides from the lecture

$$(37-1) \cdot (41-1) = 1440$$

$$\gcd(17, 1440) = 1$$

$$17 \cdot 593 \% 1440 = 1$$

$$d_a = 593$$

48.5.b Try encrypting 423. Use the algorithm for fast modular exponentiation. How many times during the recursive execution is the *if* k is odd case encountered?

5

48.5.c Decrypt the number obtained above, how many times odd and even?

Worked, 17 even 5 odd

48.6 Why is cryptopographically secure hash function used in connection with RSA digital signatures?

It is a way to secure a signature and will make it harder to forge due to not only needing to crack the key but also have to make the hash correct too.

48.7 With RSA why would you never use the value 2 as one of the two primes p and q

Due to it would be very easy to brute force the other prime.

48.8 In RSA why must the message being encrypted be a non negative integer strictly less than the modulus

Otherwise the data will be lost.

48.1 Try breaking these two encrypted messages

48.1.a Caesar cipher in english

YMNX HWDUYTLWFR NX JFXD YT IJHNUMJW.

THIS CRXPTOGRMZM IS EZSX TO DECIPHERB - shift 20

48.1.b Decrypt mono-alphabetic cipher

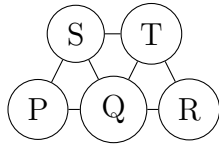
TOWWJPHJC ZY RXW PHOTWYR ZYPHJC ZJ RXW SFOPC. UFYR
FB ZR ZY QFIWOWC SZRX ZQW RXFMYHJCY FB BWWR CWWD.
GREENLAND IS THE LARGEST ISLAND IN THE WORLD. MOST OF
IT IS COVERED WITH ICE THOUSANDS OF FEET DEEP.

49 Uge

49.1 Why in RSA is it necessary that $\gcd(e_A, (p_A-1)(q_A-1)) = 1$?

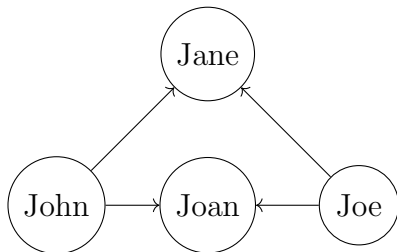
Because otherwise it would not be able to get the information back due to some values will not result in the message coming back

49.2 Draw the graph representing the road system in the figure below, and write down the number of vertices, the number of edges and the degree of each vertex



49.3 On Twitter:

49.3.a John follows Joan, Jean and Jane; Joe follows Jane and Joan; Jean and Joan follow each other. Draw a diagraph illustrating these follow relationships between John, Joan, Jane and Joe.



- 49.3.b Twitter has 313 million active users (June 2016, based on Twitter Inc.) Imagine you would like to store the diagraph for the follow relationships in an adjecency matrix that uses 4 bytes per entry on your new laptop which has 64 gb of RAM. Is this feasible

$$\begin{aligned}
 &313000000 \cdot 313000000 \\
 &\text{Entries: } 97969 \cdot 10^{12} \\
 &97969 \cdot 10^{12} \cdot 4 \\
 &3.91876 \cdot 10^{17} \text{ Bytes} \\
 &3.91876 \cdot 10^{17} \cdot 0.0000000009 \\
 &36 \cdot 10^6 \text{ gb}
 \end{aligned}$$

It would use 36 million gb of data

- 49.3.c The municipality of Odense has a population of 200000 people. Let G be the graph where the meaning of an edge from vertex i to j is "person i is friends with person j ". Imagine you would like to store the adjacency matrix for this graph for the relationships in a matrix representation that ises 4 bytes per entry on your new lapto which has 64 GB of RAM. Is this feasible?

$$\begin{aligned}
 &200000 \cdot 200000 \\
 &40 \cdot 10^9 \text{ entries} \\
 &120 \cdot 10^9 \text{ bytes} \\
 &120 \cdot 10^9 \cdot 0.0000000009 \\
 &108
 \end{aligned}$$

It would use 108 gb of ram

- 49.4 Consider the following six graphs (note tat the nodes do not have labels).

- 49.4.a How many walks of length 3 formthe red vertex to the green vvertex are there in graph 3?

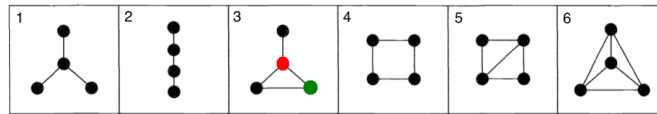


Figure 8

49.4.b How many paths from the red vertex to the green vertex are there in graph 3

2

49.4.c How many shortest paths from the red vertex to the green vertex are there in graph 3?

1

49.4.d For each of the graphs: what is the longest of all pairwise shortest paths?

- 2
- 3
- 3
- 4
- 5
- 5

49.4.e Give an adjacency matrix for graph 1. Can there be different adjacency matrices for the same graph? If so name a second adjacency matrix for graph 1. Can you find two different adjacency matrices for graph 6?

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$
 Its possible to move the second row up and down. The same argument goes for number 6

49.5 Let A be an adjacency matrix. In the lecture you learned that the ij -entry of A^k is the number of different walks from vertex i to vertex j using exactly k edges

49.5.a What is the interpretation of ij -entry of the matrix $A^1 + A^2 + A^3$?

If a walk exists with all 3 lengths it would be 6 otherwise it can be lower if a path does not exist in the given length.

49.5.b Complete the following sentence with the missing expression: In a graph G with adjacency matrix A , vertex i and j are connected if and only if ... > 0 .

ij entry has a value

49.1 Find four different square roots of 1 modulo 143, i.e., numbers which multiplied by themselves modulo 143 give 1 (and which are at least 0 and less than 143). You may consider writing a simple program for finding them.

12, 131, 142, 144

49.2 Try executing the Miller-Rabin primality test on 11, 15, and 561.

49.2.a What types of numbers are they?

11 is prime

15 is composite

561 is Carmichael number

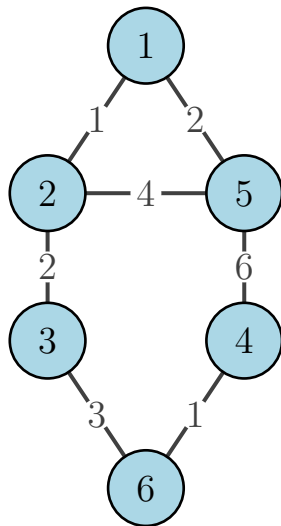
49.2.b Which numbers showed it was a composite?

15 was showed by 9

561 was showed by 35

50 Uge

50.1 Let the following weighted graph G (from the lecture slides, weights are depicted in red) be given:



$$D = \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix} & \begin{pmatrix} 0 & 1 & 3 & 7 & 2 & 6 \\ 1 & 0 & 2 & 6 & 3 & 5 \\ 3 & 2 & 0 & 4 & 5 & 3 \\ 7 & 6 & 4 & 0 & 6 & 1 \\ 2 & 3 & 5 & 6 & 0 & 7 \\ 6 & 5 & 3 & 1 & 7 & 0 \end{pmatrix} \end{matrix}$$

50.1.a How many shortest path in G are of length 6? Name them.

1 - 6
4 - 5
2 - 4

50.1.b How long is the longest of all pairwise shortest paths in the graph? Are there several longest shortest paths?

7
1 - 4
5 - 6

50.1.c How many paths in G are of length 6? (Note: a path does not necessarily need to be a shortest path.) Name them.

18 because there exists path from every point to another with the length of 6

50.2 Assume in this exercise that all weights on edges are non-negative values.

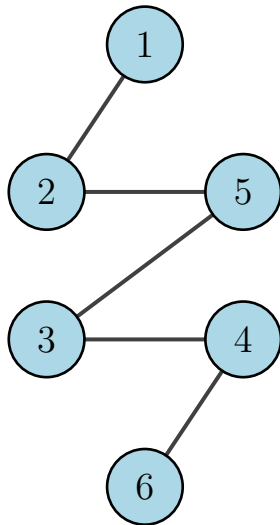
50.2.a In a graph G with $n = 6$ vertices, how many matrix-matrix multiplication operations are needed in the worst case in order to compute the distance matrix D , when the method of repeated squaring is used to compute D

$\log_2(6 - 1) = 1.61$ - so two operations

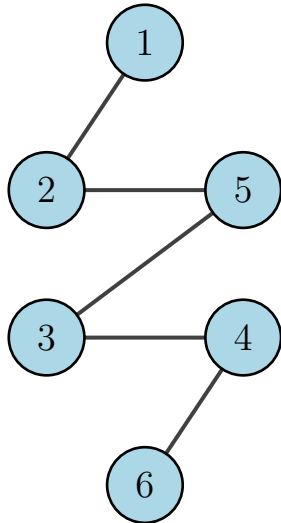
50.2.b In a graph G with $n = 200$ vertices, how many matrix-matrix multiplications are needed in the worst case in order to compute the distance matrix D , when the method of repeated squaring is used to compute D ?

$\log_2(199) = 5.3$ - so 6 operations

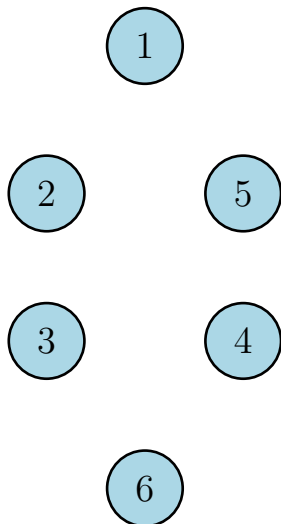
50.2.c Can you find a graph G with $n = 6$ vertices for which $W^4 \neq W^5$? if so depict it



50.2.d Can you find a graph G with $n = 6$ vertices for which $W^5 \neq W^6$? if so depict it



50.2.e Can you find a graph G with $n = 6$ vertices for which $W^1 = W^2$? if so depict it



50.2.f What is the computational runtime in order to compute the distance matrix D for a graph G with n vertices if the method of repeated squaring is used to compute D ?

$O(\log_2 n - 1)$

50.3 Consider the following molecule (it's called 2,3-Dimethylhexane)

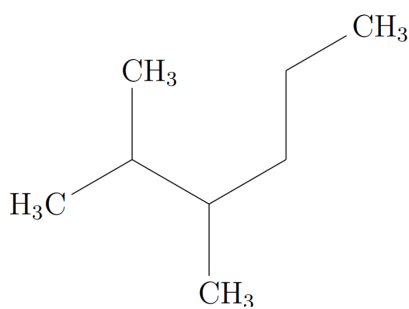
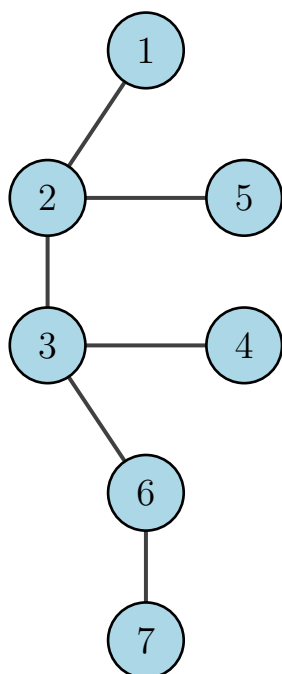


Figure 9

50.3.a How many carbon atoms does this molecule have?

8 carbons

50.3.b Draw the graph G corresponding to the carbon backbone of the molecule



50.3.c Give the edge weight matrix W for the graph G

$$W = \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix} & \begin{pmatrix} \infty & 1 & \infty & \infty & \infty & \infty & \infty \\ 1 & \infty & 1 & \infty & 1 & \infty & \infty \\ \infty & 1 & \infty & 1 & \infty & \infty & \infty \\ \infty & \infty & 1 & \infty & \infty & \infty & \infty \\ \infty & 1 & \infty & \infty & \infty & \infty & \infty \\ \infty & \infty & 1 & \infty & \infty & \infty & 1 \\ \infty & \infty & \infty & \infty & \infty & 1 & \infty \end{pmatrix} \end{matrix}$$

50.3.d Use your brain or the Java program ShortestPaths.java to infer the distance matrix.

$$W = \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix} & \begin{pmatrix} 2 & 1 & 2 & 3 & 2 & 3 & 4 \\ 1 & 2 & 1 & 2 & 1 & 2 & 3 \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 3 & 2 & 1 & 2 & 3 & 2 & 3 \\ 2 & 1 & 2 & 3 & 2 & 3 & 4 \\ 3 & 2 & 1 & 2 & 3 & 2 & 1 \\ 4 & 3 & 2 & 3 & 4 & 1 & 2 \end{pmatrix} \end{matrix}$$

50.3.e What is the Wiener Index $W(G)$

$$W(G) = 0.5 \cdot 106 = 53$$

50.3.f How many shortest paths of length $3i \rightarrow \dots \rightarrow j$ with $i < j$ are in G

6

50.3.g Using Wiener's method for predicting the boiling point, what is your prediction for 2,3-Dimethylhexane?

$$n = 8$$

$$t_0 = 745.42 \cdot \log_{10}(n + 4.4) - 689.4 = 125.66$$

$$w_0 = \frac{1}{6} \cdot (n + 1) \cdot n \cdot (n - 1) = 84$$

$$p_0 = n - 3 = 5$$

$$p = 6$$

$$t_B = t_0 - \left(\frac{98}{n^2}(w_0 - W(G)) + 5.5 \cdot (p_0 - p)\right) = 96.85$$

50.4 Assume in this exercise that all weights on edges are non-negative values. Prove the following theorem stated on the slides

If G is a weighted graph with edge weight matrix W , and vertices with indices $1, \dots, n$ then for each positive integer k the ij -th entry of

$$W^k = W \odot W \odot \dots \odot W$$

- k times

is the length of the shortest path from i to j using maximally k edges. Prove this theorem by induction over k

For a graph with two connected vertices, be multiplying the matrix, it will only contain a number larger than 0 if there is at least two edge connected to the vertice. If more is connected it will create a number equal to the number of path with the given length.