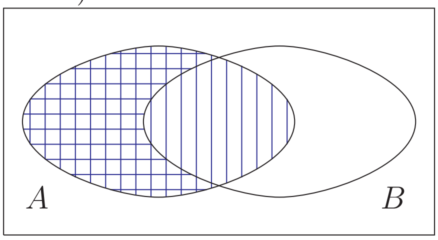
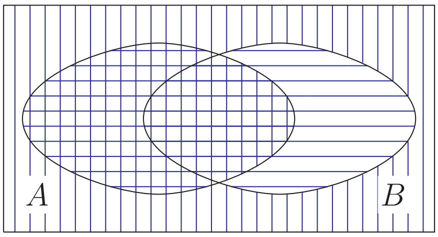
Fundamentele Informatica 1
Uitwerkingen Opgaven

1. zie *tentamen 16 december 2003*:
$A - (A - B) = A \cap B$.



A is weergeven met vertikale strepen, $A-B$ is het gedeelte dat (ook) horizontaal gestreept is. $A - (A - B)$ is vertikaal gestreept, maar *niet* horizontaal gestreept. Dus precies de doorsnede.

2a.



Horizontaal $A \cup B$, verticaal $A \cup B^c$. De doorsnede is dubbel gearceerd, en dat is inderdaad A.

3. Equivalent wil zeggen dat als één van de beweringen geldt, ze allemaal moeten gelden.

Om een gelijkheid $X = Y$ te bewijzen, laten we zien dat $X \subseteq Y$ en dat $Y \subseteq X$. Een inclusie $X \subseteq Y$ wordt als volgt beredeneerd: we laten zien dat élk element van X ook in Y zit. Dit ziet er dus uit als: 'stel $x \in X$' bla.. bla .. 'dus $x \in Y$'.

(i) Beredeneer: als $A \subseteq B$ dan $A \cap B = A$, ook genoteerd als $A \subseteq B \implies A \cap B = A$.
Dat doen we door aan te tonen dat zowel $A \cap B \subseteq A$ als $A \subseteq A \cap B$ als *gegeven* is dat $A \subseteq B$.
Stel $x \in A \cap B$, dat betekent dat $x \in A$ (en $x \in B$ maar dat hoeven we niet te weten). Het gegeven hebben we niet gebruikt: $A \cap B \subseteq A$ geldt altijd!
Andere inclusie. Stel $x \in A$. Gegeven is dat $A \subseteq B$, dus ook $x \in B$. Omdat x zowel in A als in B zit geldt $x \in A \cap B$.

(ii) Beredeneer: als $A \cap B = A$ dan $A \subseteq B$.
Stel $x \in A$. Vanwege de gelijkheid $A \cap B = A$ geldt dus $x \in A \cap B$ en daarom $x \in B$. Dat wilden we weten.

Uit (i) en (ii) volgt beweringen $A \subseteq B$ en $A \cap B = A$ zijn equivalent, oftewel $A \subseteq B$ dan en slechts dan als $A \cap B = A$; oftewel
$A \subseteq B \iff A \cap B = A$.

Op gelijke wijze $A \subseteq B \iff A \cup B = B$.

Alternatief $A \subseteq B \implies A \cap B = A \implies A \cup B = B \implies A \subseteq B$.

4a. Van de eerste taal is het twijfelachtig of λ er toe behoort; het is goed mogelijk om dat als representatie van het getal 0 op te vatten. Verder kun je ook 001 als representatie van 1 lezen. We nemen hier de 'conservatieve' interpretatie.

$K = \{\ 0, 11, 110, 1001, 1011, 1100, \dots\ \}$

$L = \{\ \lambda, 0, 1, 01, 10, 11, 010, 011, 101, 110, \dots\ \}$

4b. $K \cap L$ bevat 0 en 11110.

$K - L$ bevat 1001 en 10010.

$L - K$ bevat λ en 11111 (of 01011: wel drievoud maar geen representatie).

$(K \cup L)^c$ bevat 00 en 10000 (of 00000).

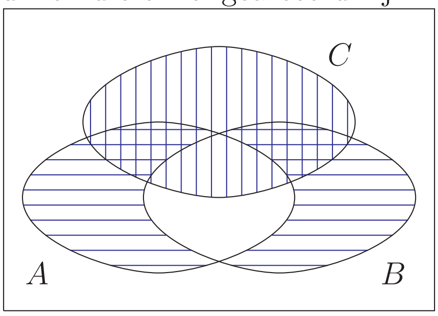
5. *tentamen 30 juli 2004*

6. We maken gebruik van 'substitutie': als in een expressie een deel vervangen wordt door een equivalente expressie, dan is het resultaat equivalent met de oorspronkelijke expressie. Met andere woorden, we kunnen regels toepassen op delen van de expressie. Associativiteit zegt dat $x@(y@z) = (x@y)@z$ en met $x = 1$, $y = (2@3)$ en $z = 4$ volgt volgt $1@((2@3)@4) = (1@(2@3))@4$. Gebruik nu substitutie (en blijf doorgaan ...).

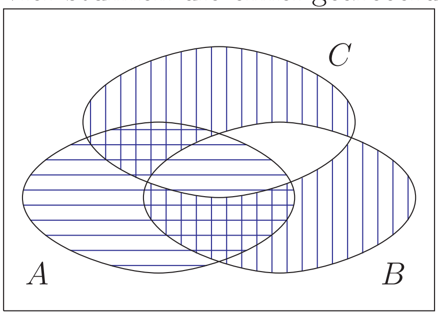
$(1@((2@3)@4)) @(5@6) =$
$((1@(2@3))@4) @(5@6) =$
$(1@(2@3))@(4@(5@6)) =$
$((1@2)@3)@(4@(5@6)) =$
$(1@2)@(3@(4@(5@6))) =$
$1@(2@(3@(4@(5@6)))) =$

Op welke delen passen we associativiteit toe? En hoe zien de bomen bij de expressies eruit?

7a. Maak eerst een Venn diagram van de linkerzijde. Horizontaal $A \oplus B$, vertikaal C. Het gebied van $(A \oplus B) \oplus C$ bestaat uit de vier stukken die enkel gearceerd zijn.



Dan de rechterzijde. Horizontaal A, vertikaal $B \oplus C$. Het gebied van $A \oplus (B \oplus C)$ bestaat uit de vier stukken die enkel gearceerd zijn.



De twee expressies geven hetzelfde gebied aan en zijn dus gelijk. Het symmetrisch verschil van drie verzamelingen bestaat uit de elementen die in een oneven aantal van die verzamelingen zitten (namelijk in precies één of in alledrie).

7b. Tja. De definitie van het symmetrisch verschil is 'symmetrisch', we kunnen A en B daarin verwisselen. Eigenlijk volgt de bewering uit de commutativiteit van vereniging $A \oplus B = A \backslash B \cup B \backslash A = B \backslash A \cup A \backslash B = B \oplus A$

7c. Gegeven: $A \oplus B = A \oplus C$.

Te bewijzen: $B = C$.

We laten zien dat $B \subseteq C$, de andere inclusie is op dezelfde manier te bewijzen.
Kies $x \in B$. We onderscheiden twee gevallen.
Als $x \in A$, dan $x \notin A \oplus B = A \oplus C$. Omdat x in A zit, maar niet in $A \oplus C$, moet $x \in C$.
Als $z \notin A$, dan $x \in A \oplus B = A \oplus C$. Omdat x niet in A zit, maar wel in $A \oplus C$, moet $x \in C$.

Er is ook een algebraische manier om dit te bewijzen. Dan moeten we twee regels gebruiken: $A \oplus A = \varnothing$, en $\varnothing \oplus A = A$.

Er geldt dan: als $A \oplus B = A \oplus C$ dan $B = \varnothing \oplus B = (A \oplus A) \oplus B = A \oplus (A \oplus B) = A \oplus (A \oplus C) = (A \oplus A) \oplus C = \varnothing \oplus C = C$, oftewel $B = C$.

8a. *Uitgewerkt tentamen is beschikbaar.*

8b. Moeten we wel eerst $B - A$ schrijven als $B \cap A^c$, anders laten de regels ons in de steek.

$$
\begin{array}{rl}
(A \cup B^c) \cup (B - A) = & \\
(A \cup B^c) \cup (B \cap A^c) = & d \\
((A \cup B^c) \cup B) \cap ((A \cup B^c) \cup A^c) = & 2{\times}a \\
(A \cup (B^c \cup B)) \cap (A \cup (B^c \cup A^c)) = & 2{\times}c \\
(A \cup (B \cup B^c)) \cap (A \cup (A^c \cup B^c)) = & C{,}a \\
(A \cup U) \cap ((A \cup A^c) \cup B^c) = & i{,}C \\
U \cap (U \cup B^c) = & 2{\times}c \\
(B^c \cup U) \cap U = & 2{\times}i \\
 & U
\end{array}
$$

a: associatief; c: commutatief; C: complement; d: distributief; i: identiteit;

Dan gebruiken we distributiviteit.

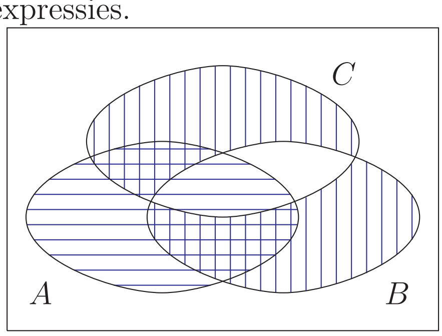
$$
\begin{array}{rl}
[\,(A \cup B^c) \cap C\,] \cup [\,(B - A) \cap C\,] = & 2\times c \\
[\,C \cap (A \cup B^c)\,] \cup [\,C \cap (B - A)\,] = & d \\
C \cap [\,(A \cup B^c) \cup (B - A)\,] = & \\
C \cap U = & i \\
 & C
\end{array}
$$

Dit wordt véél korter als we aannemen dat van elke regel ook de 'commutatieve' versie aanwezig is, dus bijvoorbeeld $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ en $U \cup A = U$. Op tentamen doen we dáár niet moeilijk over.

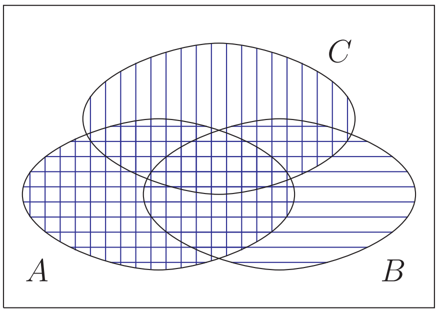
9a. Nee, dat volgt niet. Zowel $A \cup B$ als $A \cup C$ bevatten ieder A, en de overige elementen zijn uit respectievelijk $B - A$ en $C - A$. Er geldt $B - A = C - A$, maar $A \cap B$ en $A \cap C$ hoeven niet gelijk te zijn.

Kies bijvoorbeeld $A = \{a\}$, $B = \{b\}$ en $C = \{a, b\}$ om te laten zien dat de gelijkheid niet geldt.

9b. Teken een Venn diagram voor elk van de twee expressies.



Horizontaal A, vertikal $B \oplus C$, dus voor $A \cup (B \oplus C)$ zijn we geinteresseerd in alles wat gearceerd is.



Horizontaal $A \cup C$, vertikal $A \cup C$, dus voor $(A \cup B) \oplus (A \cup C)$ zijn we geinteresseerd in alles wat enkel gearceerd is.

De twee gebieden zijn bij lange na niet hetzelfde.

Als tegenvoorbeeld kunnen we kiezen $A = \{1\}$, $B = C = \varnothing$. Dan $A \cup (B \oplus C) = \{1\}$, terwijl $(A \cup B) \oplus (A \cup C) = \varnothing$.

10. We voeren onofficiele notatie in. Dat is handig want we kunnen daarmee stukken van het Venn diagram benoemen: n_{arw}, met $a, r, w \in \{0, 1, *\}$ is het aantal elementen in een verzameling waarin air-conditioning A, radio R, power windows W, respectievelijk niet meedoet (0), wel meedoet (1) of ongespecifieerd ($*$) [is daar iets van te snappen?]. Bijvoorbeeld: $n_{1*0} = n(A - W)$, wel air-conditioning, geen power windows [wat dat ook moge zijn], en radio onbekend.

Gegeven zijn de volgende getallen $n_{1**} = n(A) = 15$, $n_{*1*} = n(R) = 12$, $n_{**1} = n(W) = 11$, $n_{1*1} = n(A \cap W) = 5$, $n_{11*} = n(A \cap R) = 9$, $n_{*11} = n(R \cap W) = 4$, $n_{111} = n(A \cap R \cap W) = 3$. Oh, én $n_{***} = n(U) = 25$ het totaal aantal auto's.

Volgens de 'formule van inclusie en exclusie' vinden we $n(A \cup R \cup W) = 15 + 12 + 11 - 5 - 9 - 4 + 3 = 23$.

Dus voor de overige parten van het Venn diagram geldt $n_{101} = n_{1*1} - n_{111} = 5 - 3 = 2$, $n_{110} = n_{11*} - n_{111} = 9 - 3 = 6$, $n_{011} = n_{*11} - n_{111} = 4 - 3 = 1$.

$n_{100} = n_{1**} - n_{110} - n_{101} - n_{111} = 15 - 6 - 2 - 3 = 4$ [of kan dat korter?], en op dezelfde manier $n_{010} = 2$, $n_{001} = 5$.

Dan tenslotte $n_{000} = n_{***} - n(A \cup R \cup W) = 2$. Hiermee zijn alle parten van het Venn-diagram geteld, en kunnen we de opgave maken.

(a) only power windows $n_{001} = 5$ (b) only air-conditioning; $n_{100} = 4$ (c) only radio; $n_{010} = 2$ (d) $n_{011} = 1$ [uitwerking Schaum zegt wat anders?] (e) air-conditioning and radio, but not power windows; $n_{110} = 6$ (f) only one of the options; optellen $5 + 4 + 2 = 11$ (g) at least one option; $n(A \cup R \cup W) = 23$ (h) none of the options. $n_{000} = 2$

11. Volgens Theorem 1.9 geldt $n(A \cup B) = n(A) + n(B) - n(A \cap B)$. Dit blijft gelden als we B vervangen door $(B \cup C)$: $n(A \cup B \cup C) = n(A) + n(B \cup C) - n(A \cap (B \cup C))$. Gebruik nu distributiviteit $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, en gebruik Theorem 1.9 tweemaal:
$n(A \cup B \cup C) = \ldots$
$= n(A) + n(B \cup C) - n((A \cap B) \cup (A \cap C)) = n(A) + n(B) + n(C) - n(B \cap C) - n(A \cap B) - n(A \cap C) + n((A \cap B) \cap (A \cap C))$.

Net wat we zoeken, want $(A \cap B) \cap (A \cap C) = A \cap B \cap C$.

13a. $\mathcal{P}(\{0,1\}) = \{\ \varnothing, \{0\}, \{1\}, \{0,1\}\ \}$, vier elementen. $\mathcal{P}(\mathcal{P}(\{0,1\}))$ heeft er $2^4 = 16$. Om het een beetje leesbaar te houden geven we de verzamelingen in de machtsverzamelingen aan met vierkante haakjes. $\{\ \varnothing,\ [\varnothing],\ [\{0\}],\ [\varnothing, \{0\}],$
$[\{1\}],\ [\varnothing, \{1\}],\ [\{0\}, \{1\}],\ [\varnothing, \{0\}, \{1\}],$
$[\{0,1\}],\ [\varnothing, \{0,1\}],\ [\{0\}, \{0,1\}],$
$[\varnothing, \{0\}, \{0,1\}],$
$[\{1\}, \{0,1\}],\ [\varnothing, \{1\}, \{0,1\}],$
$[\{0\}, \{1\}, \{0,1\}],\ [\varnothing, \{0\}, \{1\}, \{0,1\}]\ \}$

13b. Vervang in het antwoord hierboven '0' door '$\varnothing$' en '1' door '$\{\varnothing\}$'. Tja.

14a. $\kappa_{A^c}(x) = 1 - \kappa_A(x)$

14b. $\kappa_{A \cap B}(x) = \kappa_A(x) \cdot \kappa_B(x)$
$\kappa_{A \cup B}(x) = \kappa_A(x) + \kappa_B(x) - \kappa_A(x) \cdot \kappa_B(x)$ (de één of de ander minus de dubbeltelling)
Als we ons laten inspireren door De Morgan vinden we hetzelfde via het eerste onderdeel en $\kappa_{A \cup B}(x) = 1 - (1 - \kappa_A(x))(1 - \kappa_B(x))$

15. Schaum p. 34/35

16.

16f. 'eerst terug, dan heen' $R^{-1} \circ R = \{\ (2,2), (2,3), (2,4), (3,2), (3,3), (3,4), (4,2), (4,3), (4,4)\ \}$.
'eerst heen, dan terug' [mmm, dat staat niet in de opgave] $R \circ R^{-1} = \{\ (1,1), (1,3), (3,1), (3,3)\ \}$.

17a. Antisymmetrisch en transitief. En irreflexief, niet reflexief. Let op: het komt *niet* voor dat zowel $x < y$ én $y < x$ en daarom is de relatie antisymmetrisch.

17b. Wél reflexief (al zegt Schaum van niet) want x^2 is nu eenmaal een kwadraat. Symmetrisch want $xy = yx$. Ook transitief. Stel $xy = p^2$ en $yz = q^2$ dan is $xz = (pq/y)^2$. Omdat dit kwadraat een geheel getal is, is ook $\frac{pq}{y}$ geheel (!) en dus is xz een kwadraat van een geheel getal.

Deze transitiviteit kan beter 'aangevoeld' worden als volgt. Een getal is een kwadraat desdals elke priemdeler een even aantal keer als factor voorkomt. Kies een priem p. Omdat xy en yz kwadraten zijn komt p een even aantal keer voor in beide getallen. Als p een [on]even aantal keer voorkomt in y dan moet p ook een [on]even aantal keer voorkomen in y en in z, en dus een even aantal keer in yz.

Omdat dit voor alle priem p geldt, is yz een kwadraat.

Een reflexieve, symmetrische en transitieve relatie heet een equivalentierelatie.

Lemma. $\sqrt{2}$ is geen breuk.

bewijs. Stel $\sqrt{2} = \frac{p}{q}$ met p, q geheel. Dan $p^2 = 2q^2$. De linkerzijde heeft een even aantal factoren 2, de rechterkant een oneven aantal.

17c. $R = \{ (1,9), (2,8), \ldots (9,1) \}$

Symmetrisch (dus niet antisymmetrisch). Verder niet reflexief $(1,1) \notin R$, niet transitief $(1,9), (9,1) \in R$, niet irreflexief $(5,5) \in R$. De relatie is eindig, dwz. er zijn maar eindig veel elementen.

17d. De relatie is precies gelijk aan $\{ (6,1), (2,2) \}$. Is daarom wél transitief.

17e. a. $\{ (x,y) \mid x \geq y-2 \}$, zodat er tussen x en y nog een getal kan liggen.
b. In dit geval de relatie zelf, omdat de relatie transitief is geldt $R^2 \subseteq R$, omdat de relatie óók reflexief is geldt $R = R \circ \mathrm{id} \subseteq R^2$.
c. $\{ (1,1), (2,2), \cdots, (9,9) \}$.
d. $\{ (2,2) \}$.

18. Een relatie is een verzameling. De doorsnede van twee relaties bestaat dus uit de paren die in beide relaties zitten.

Stel R en S zijn symmetrisch. Kies $(x,y) \in R \cap S$, dan (x,y) in zowel R als S. Deze zijn beide symmetrisch, (y,x) in zowel R als S. Daarmee is $(y,x) \in R \cap S$ en is $R \cap S$ symmetrisch.

Stel R en S zijn symmetrisch. Kies $(x,y) \in R \cup S$, dan (x,y) in R of in S. Deze zijn beide symmetrisch, dus (y,x) in R of in S afhankelijk van waar (x,y) gevonden is. Daarmee is $(y,x) \in R \cup S$ en is $R \cup S$ symmetrisch.

Als R en S transitief zijn, hoeft $R \cup S$ dat niet te zijn: $R = \{ (1,2) \}$, $S = \{ (2,3) \}$.

Als R en S antisymmetrisch zijn, hoeft $R \cup S$ dat niet te zijn: $R = \{ (1,2) \}$, $S = \{ (2,1) \}$.

19a. Stel $R^{-1} \circ R \subseteq 1_B$. We laten zien dat R functioneel is. Kies dus $(x,y), (x,z) \in R$. Dan $(y,x) \in R^{-1}$, $(x,z) \in R$, dus $(y,z) \in R^{-1} \circ R$. Omdat deze laatste relatie volgens de aanname bevat is in 1_B, moet $y = z$, waarmee bewezen is dat R functioneel is.

Ook het omgekeerde moet bewezen worden, dat is vrijwel dezelfde redenatie achteruit. Stel R is functioneel. Kies $(x,z) \in R^{-1} \circ R$, er is dus een $y \in A$ met $(x,y) \in R^{-1}$ en $(y,z) \in R$. Maar dan $(y,x), (y,z)$ allebei in R. Omdat R functioneel is moet $x = z$, daarom is het paar $(x,z) = (x,x)$ een element van 1_B.

21a. Een functie h is injectief als uit $h(x) = h(y)$ volgt dat $x = y$, oftwel er zijn geen twee (verschillende) originelen met hetzelfde beeld.

Stel nu $(g \circ f)(x) = (g \circ f)(y)$ dat wil zeggen $g(f(x)) = g(f(y))$. Omdat g injectief is geldt $f(x) = f(y)$. Omdat f injectief is geldt $x = y$. Daarmee is duidelijk dat $g \circ f$ injectief is.

22a. Dit zijn alle getallen waarvan de binaire ontwikkeling eindigt in *precies* twee enen, dus 11, of van de vorm $x011$, met x een string in $\{0,1\}^*$ beginnend met een 1. Zo'n getal is een achtvoud plus 3, dus de verzameling $\{3, 11, 19, \ldots\} = \{ 8n+3 \mid n \in \mathbb{N} \}$.

23a. In het algemeen geldt, voor $Y \subseteq B$ dat $f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$.

Kies $X \in V$, en kijk naar $y = f(x)$. Dan $y \in f(V)$ en (per definitie) $x \in f^{-1}(f(V))$, omdat $f(x) \in V$. Daarmee is de inclusie $V \subseteq f^{-1}(f(V))$ bewezen.

Bij een injectieve functie verandert dit in gelijkheid. Stel $x \in f^{-1}(f(V))$ dus $f(x) \in f(V)$. Dat wil zeggen $f(x) = f(y)$ voor een $y \in V$. Nu f injectief is, moet gelden $x = y$ en daarmee $x \in V$. Dit bewijst de omgekeerde inclusie.

24a. $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, $F_7 = 13$, $F_8 = 21$, $\ldots$.
$\sum_{k=1}^{4} F_{2k} = F_2+F_4+F_6+F_8 = 1+3+8+21 = 33$.

24b. $\sum_{k=0}^{n} 1 = n+1$, $n+1$ keer het getal 1 optellen.

24c. Alle échte veelvouden zijn verboden, dus alle getallen die te schrijven zijn als $x \cdot y$ met x en y ongelijk 1. Dus we sluiten alle getallen in V_n $(n \geq 2)$ uit, behalve misschien n zelf (als n zelf geen veelvoud is):
$\mathbb{P} - \bigcup_{n=2}^{\infty}(V_n - \{n\})$

24d. De rijen worden genummerd door i, de kolommen door j, steeds van 1 tot n. Rechtsboven de diagonaal geldt $i < j$. Maak eerst een sommatie die de rijen optelt (lopend over de waarden van i) en per rij de elementen (lopend over de geschikte waarden van j) $\sum_{i=1}^{n} \sum_{j=i+1}^{n} a_{ij}$.

25a. Aanwijzing: eerst proberen zonder de mintekens.
$\sum_{i=1}^{n}(-1)^{i+1} i^2 = (-1)^{n+1} \sum_{i=1}^{n} i$

25b. $\sum_{i=1}^{n} \frac{1}{i \cdot (i+1)} = \frac{n}{n+1}$

26. Een functie van $\mathbb{N}$ naar $\mathbb{Z}$. Stuur de even getallen naar hun halve waarde, en de oneven getallen naar de helft negatief (afgerond): $0 \mapsto 0$, $1 \mapsto -1$, $2 \mapsto 1$, $3 \mapsto -2$, $4 \mapsto 2$, $\ldots$ Algemeen $2n \mapsto n$, en $2n+1 \mapsto -n-1$ voor $n \geq 0$. Omdat elk element van $\mathbb{Z}$ precies één keer beeld is, is dit een bijectie. Zie dictaat.

27. *Uitgewerkt tentamen is beschikbaar.*

28. Een simpel pad is een pad met allemaal verschillende knopen. Een *trail* is een pad met alle takken verschillend.

Officieel is een pad een reeks afwisselende knopen en takken, maar die notatie is alleen relevant wanneer de graaf parallelle takken heeft. Anders loopt de tak gewoon tussen de aanliggende knopen. We gebruiken daarom (meestal) een verkorte notatie en geven alleen het rijtje knopen.

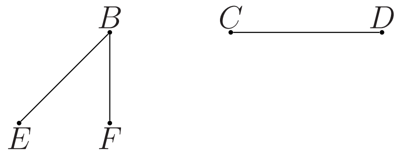
In de definitie van Schaum moeten we overigens een woord wijzigen: '... where each edge e_i *connects* the vertices v_{i-1} and v_i ...'. Het is anders mogelijk om ter weerszijden van een tak twee keer dezelfde knoop te kiezen! (Dat mag alleen als de tak een lus (*loop*) is.) Op de uitwerking in Schaum is nog wat op te merken.

28. (a) De stelling klopt inderdaad: de som der graden $2+4+3+2+2+2+3+2 = 20$ is twee maal 10, het aantal takken.

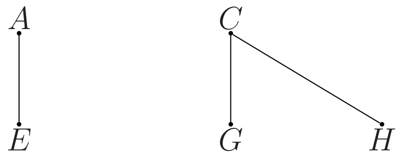
(c) Een *trail* mag inderdaad een knoop meerdere keren aandoen, zoals ook blijkt uit de uitwerking in Schaum. Ook hoeven we niet te stoppen wanneer C bereikt is, dus $BEABGCHDC$ is een mogelijke oplossing. Jeroen vond 18 trails.

29. Met het noemen van de cycle $ABEA$ worden eigenlijk zes cycles geïdentificeerd, steeds met een ander beginpunt op het genoemde pad: $ABEA$, $BEAB$, en $EABE$, en de drie cykels in omgekeerde richting: $AEBA$, $BAEB$, $EBAE$. Als *graaf* is dat steeds hetzelfde rondje van drie takken, maar als *pad* niet!

30. 'generated by' betekent dat we een geïnduceerde subgraaf moeten bepalen, dus alleen de genoemde knopen met al hun onderlinge takken. We vinden zo



en voor b:



Dit zijn natuurlijk isomorfe grafen.

31. Sloane A001349
Voor een plaatje (tot en met vijf) http://mathworld.wolfram.com/ConnectedGraph.html

32. Twee verschillende paden kunnen samengevoegd worden tot een gesloten pad. Dat is nog geen cycle: een cycle mag geen knopen twee keer aandoen, en het bewijs moet uitleggen hoe we de dubbele knopen gaan verwijderen.

Maar dan moet nog uitgelegd worden wat *distinct paths* zijn. Bekijk de deelgraaf met alleen de takken EA, AB en BF. Dat is een 'lijngraaf' waar geen cycle te vinden is. Toch zijn er twee verschillende paden van A naar B: $AEAB$ en $ABFB$.

Ik stel voor: Suppose that a graph G contains two distinct *simple* paths from a vertex u to a vertex v. Then G has a cycle.

Bewijs. Door het tweede pad achterstevoren aan het eerste te plakken ontstaat een gesloten pad C, van u via v naar u terug. Omdat de oorspronkelijke paden verschillend zijn, is er een tak, zeg $\{x, y\}$, dat maar op één van de paden ligt, en dus op C maar één keer voorkomt. Door de tak $\{x, y\}$ uit C weg te laten kunnen we een pad van y naar x maken. Volgens Theorem 8.2 is er nu ook een simpel pad S van y naar x. We mogen aannemen dat S níet uit de tak $\{x, y\}$ bestaat, omdat het onstaat uit een pad van y naar x waarop die tak niet ligt '*by deleting unnecessary edges*'. Voeg nu aan S de tak $\{x, y\}$ toe en we vinden een echte cykel.

33a. Neem twee knopen x en y. In G zijn ze verbonden door een pad. Als dat pad de tak e niet bevat, ligt het ook in $G - e$ en zijn x en y verbonden. Als het pad e wél bevat, vervangen we e door de rest van de cycle C: dit pad verbindt dezelfde knopen als e, en mag e niet bevatten (omdat een cycle allemaal verschillende knopen heeft).

33b. Kennelijk is e een brug in G.

Als u en v in dezelfde component van $G - e$ liggen, worden ze verbonden door een pad, en zelfs door een simpel pad (zie Theorem 8.2). Verleng dat pad met de tak e en we vinden een cycle met daarop tak e. Volgens het vorige onderdeel moet de graaf $G - e$ samenhangend [*connected*] zijn. Tegenspraak, dus kunnen u en v niet in dezelfde component van $G - e$ liggen.

35b. Elk woord uit de taal dat met een b begint heeft oneven lengte (en bestaat geheel uit b's). Equivalent met deze bewering is dat elk woord uit L ofwel met een a begint ofwel oneven lengte heeft.

Er zijn twee regels, één die een a vooraan toevoegt, de ander die twee b's achteraan zet. Als een woord niet met een b begint, is de eerste regel nooit toegepast, en is herhaald regel twee toegepast op beginletter b. Dat geeft een oneven aantal b's.

Formeel: *basis.* a begint met een a, b heeft oneven lengte.

inductiestap. Onder de aanname dat x aan de eigenschap voldoet, bewijzen we de eigenschap voor ax en xbb apart.

- ax begint met een a (de aanname wordt hier niet gebruikt).
- We onderscheiden twee gevallen; als x met een a begint, is aan de eigenschap voldaan omdat dan ook xbb met een a begint. Anders heeft x oneven lengte, maar dan heeft ook xbb die eigenschap.

35c. L bestaat uit woorden van de vorm b^n met $n \geq 1$ oneven, of van de vorm $a^m b^n$ met $m \geq 1$, $n \geq 0$ willekeurig.

36a. Bijvoorbeeld u, x, z, y, t, r, s, w.

36b. Elke (eindige) gerichte graaf zonder cycles heeft volgens Theorem 9.3 een bron, een punt van waaruit slechts takken kunnen vertrekken. Een topologische sortering vinden van een graaf vinden we door herhaald een bron te bepalen en deze met uitgaande takken uit de graaf te verwijderen. De bronnen in de gevonden volgorde vormen een topologische sortering. (Jaah? Is dat duidelijk?)

37b. `fibo(4)` drukt hetzelfde af als `fibo(3);fibo(2)`, dus hetzelfde als `fibo(2);fibo(1);fibo(1);fibo(0)`, dus `fibo(1);fibo(0);fibo(1);fibo(1);fibo(0)` dus `babba`.

De twee basisgevallen `fibo(0)` en `fibo(1)` printen een enkel karakter, verder is de lengte van een `fibo(n)` de som van de lengtes van de twee voorgangers, net als bij de Fibonacci getallen. Dit levert de reeks $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$ beginnend bij de lengte van `fibo(0)`. Dan is de lengte van `fibo(8)` gelijk aan 34.

Eenzelfde verhaal voor de `a`'s en de `b`'s, maar dan met andere beginwaarden.

38a. $\sum_{k=1}^{n}(2k-1) = n^2$.
basis. $(n = 1)$ $\sum_{k=1}^{1}(2k-1) = 1 = 1^2$.
inductiestap. We nemen aan dat de formule waar is vooor n. Dan voor $n+1$: $\sum_{k=1}^{n+1}(2k-1) = \sum_{k=1}^{n}(2k-1)+2(n+1)-1 = n^2 + 2n + 1 = (n+1)^2$. Hetgeen te bewijzen was.

39b. We vervangen het rechterlid door $(-1)^n \cdot \frac{n(n+1)}{2}$, dat mag volgens de vorige opgave.
$\sum_{k=1}^{n}(-1)^k k^2 = (-1)^n \frac{n(n+1)}{2}$
inductiestap. We nemen aan dat de formule waar is vooor n. Dan voor $n+1$: $\sum_{k=1}^{n+1}(-1)^k k^2 = \sum_{k=1}^{n}(-1)^k k^2 + (-1)^{n+1}(n+1)^2 = (-1)^n \frac{n(n+1)}{2} + (-1)^{n+1}(n+1)^2 = (-1)^{n+1}(-\frac{n(n+1)}{2} + \frac{2(n+1)(n+1)}{2}) = (-1)^{n+1}(\frac{(n+2)(n+1)}{2})$.

40. *basis.* $(1-a)^0 = 1 \geq 1 = 1 - 0a$.
inductiestap. We gebruiken dat $1-a$ positief is. $(1-a)^{n+1} = (1-a)(1-a)^n \geq (1-a)(1-na) = 1-(n+1)a + na^2 \geq 1-(n+1)a$.

41. $(x+y)^{n+1} = (x+y)(x+y)^n = (x+y) \cdot \sum_{k=0}^{n}\binom{n}{k}(x^k y^{n-k}) = \sum_{k=0}^{n}\binom{n}{k}(x^{k+1}y^{n-k}) + \sum_{k=0}^{n}\binom{n}{k}(x^k y^{n-k+1})$. In elke term hebben x en y samen exponent $n+1$. Het totale aantal $x^k y^{n-k+1}$ is $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ gebruikmakend van de regels voor binomiaalcoëfficienten.

Maar het *hoeft* niet met inductie. Het product $(x+y)^n$ bestaat uit n factoren $(x+y)$. Uitgeschreven bestaat $(x+y)^n$ uit 2^n termen, die als we nog een gebruik maken van commutativiteit van vermenigvuldigen, er uitzien als alle strings van lengte n over $\{x, y\}$. We vegen dan alle termen met gelijke aantallen x

en y bij elkaar (commutativiteit). (Bijvoorbeeld $(x+y)^3 = xxx + xxy + xyx + \cdots + yxx + \cdots + yyy = x^3 + 3x^2y + 3xy^2 + y^3$. Wat is de constante bij de term $x^k y^{n-k}$? dat is gelijk aan het aantal keren dat we uit de n factoren $(x+y)$ in totaal k keer een x kiezen (en $n-k$ keer een y). Dat kan natuurlijk op $\binom{n}{k}$ manier!

42b. *basis* zelf nagaan. *inductiestap.* $\sum_{k=1}^{n+1} F_k = F_{n+1} + \sum_{k=1}^{n} F_k \overset{h}{=} F_{n+1} + F_{n+2} - 1 \overset{d}{=} F_{n+3} - 1$. Hierbij is bij h de inductiehypothese gebruikt, bij d de definitie van Fibonacci.

42c. *basis* $n=1$: $\sum_{k=1}^{1} F_k^2 = F_1^2 = 1 = F_1F_2$. *inductiestap.* $\sum_{k=1}^{n+1} F_k^2 = F_{n+1}^2 + \sum_{k=1}^{n} F_k^2 \overset{h}{=} F_{n+1}^2 + F_nF_{n+1} = F_{n+1} \cdot (F_{n+1} + F_n) \overset{d}{=} F_{n+1}F_{n+2}$. Hierbij zijn h en d als boven.

43b. Kies de matrix $Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Dan geldt $Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$ voor $n \geq 1$. Voor $n = 0$ geldt $Q^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, en dat is ook van de gewenste vorm, als we tenminste $F_{-1} = 1$ kiezen. Er geldt dan zelfs $F_1 = F_0 + F_{-1}$.

Omdat $Q^{2n} = Q^nQ^n$ ook bij het vermenigvuldigen van matrices, Kunnen we van de matrix de elementen bekijken: linksboven $F_{2n+1} = F_{n+1}^2 + F_n^2$ en rechtsboven $F_{2n} = F_{n+1}F_n + F_nF_{n-1}$. Die laatste waarde is gelijk aan $F_n(F_{n+1} + F_{n-1})$ en dat is, volgens de Fibonacci regel achterstevoren, $(F_{n+1} - F_{n-1})(F_{n+1} + F_{n-1}) = F_{n+1}^2 - F_{n-1}^2$.

Zonder matrices brengt de Formule van Binet uitkomst. Schrijf $\phi = \frac{1+\sqrt{5}}{2}$, en $\hat{\phi} = \frac{1-\sqrt{5}}{2}$. Er geldt $\phi^2 = \phi + 1$ en ook $\hat{\phi}^2 = \hat{\phi} + 1$, $\phi + \hat{\phi} = 1$, terwijl $\phi \cdot \hat{\phi} = -1$.

Dan $F_n = \frac{1}{\sqrt{5}}(\phi^n - \hat{\phi}^n)$, dus $F_{n+1}^2 - F_{n-1}^2 = \frac{1}{5}[(\phi^{n+1} - \hat{\phi}^{n+1})^2 - (\phi^{n-1} - \hat{\phi}^{n-1})^2] = \frac{1}{5}[\phi^{2n+2} - 2(-1)^{n+1} + \hat{\phi}^{2n+2} - \phi^{2n-2} + 2(-1)^{n-1} - \hat{\phi}^{2n-2}]$. De machten van -1 vallen tegen elkaar weg. $\phi^{2n+2} - \phi^{2n-2} = \phi^{2n}(\phi^2 - \phi^{-2})$. Hmm. $\phi^2 - \phi^{-2} = \sqrt{5}$ en $\hat{\phi}^2 - \hat{\phi}^{-2} = -\sqrt{5}$. Dus $F_{n+1}^2 - F_{n-1}^2 = \frac{1}{5}[\sqrt{5}\phi^{2n} - \sqrt{5}\hat{\phi}^{2n}] = \frac{1}{\sqrt{5}}(\phi^{2n} - \phi^{2n}) = F_{2n}$. Zucht.

43c. Dit lijkt het *Binomium van Newton* wel? Dat luidt voor matrices: $(X+I)^n = \sum_{k=0}^{n} \binom{n}{k} X^k$, waarbij I de 2×2 eenheidsmatrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is, dus $XI = IX = X$. Kies nu $X = Q$. De rechterflank van Newton is dus een matrix met $\sum_{k=0}^{n} \binom{n}{k} F_k$ rechtsboven. Wat staat op de linkerflank? Verrassing! $Q + I = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = Q^2$, en dan $(Q+I)^n = (Q^2)^n = Q^{2n}$. Die matrix heeft F_{2n} rechtsboven.

Newton geldt niet voor willekeurige matrices, dwz. de formule bevat de eenheidsmatrix I, en op die plek kan niet zomaar elke waarde staan. Matrixvermenigvuldigen is immers niet commutatief, en is dus $(X+Y)^2 = X^2 + XY + YX + Y^2$ niet zonder meer gelijk aan $(X+Y)^2 = X^2 + 2XY + Y^2$. Als X en Y commuteren, dwz. $XY = YX$, dan geldt Newton wel voor deze matrices.

Zonder matrices brengt de Formule van Binet uitkomst. Schrijf $\phi = \frac{1+\sqrt{5}}{2}$, dan $(\phi+1)^n = \sum_{k=0}^{n} \binom{n}{k} \phi^k$ volgens de formule van Newton. Maar $\phi^2 = \phi + 1$ als wortel van de vergelijking $x^2 - x - 1 = 0$, dus $(\phi+1)^n = \phi^{2n}$. Zelfde verhaal voor $\hat{\phi} = \frac{1-\sqrt{5}}{2}$.

44. *basis.* $L_2L_0 - L_1^2 = 3 \cdot 2 - 1^2 = 5 = 5(-1)^0$

inductiestap. Bij ℓ gebruiken we de definitie van de Lucas getallen, bij h de inductieaanname.

$L_{n+3}L_{n+1} - L_{n+2}^2 \overset{\ell}{=} (L_{n+1} + L_{n+2})L_{n+1} - L_{n+2}^2 = L_{n+1}^2 + L_{n+2}(L_{n+1} - L_{n+2}) \overset{\ell}{=} L_{n+1}^2 - L_{n+2}L_n \overset{h}{=} -5(-1)^n = 5(-1)^{n+1}$.

45. Machtsverheffen kan in logaritmische tijd uitgedrukt in de exponent; gebruik nu de matrix Q uit een van de vorige opgaven. Of gebruik rechtstreeks de uitdrukkingen voor F_{2n} en F_{2n+1} in termen van F_{n-1}, F_n en F_{n+1}, die het mogelijk maken om de index van te berekenen getallen ongeveer te halveren.

47a. $f(\text{blad}) = 1$, terwijl $f(\text{knoop}) = 1 + f(\text{links}) + f(\text{rechts})$. Hierbij nemen we wel aan dat de knoop zowel links als rechts een kind heeft. Misschien is het beter om de recursie-basis te laten beginnen bij een *lege* boom: $f(\text{leeg}) = 0$.

47b. De hoogte gemeten in aantal takken (zoals standaard in Schaum): $f(\text{blad}) = 0$, en $f(\text{knoop}) = \max\{f(\text{links}), f(\text{rechts})\} + 1$.

47c. Neem aan dat de waarde van een knoop met de functie w bepaald kan worden. Dan $f(\text{blad}) = w(\text{blad})$, en $f(\text{knoop}) = \max\{f(\text{links}), f(\text{rechts}), w(\text{knoop}\}$.

48a. De inductieve formule. Bekijk derangementen van n objecten $\{1, \ldots, n\}$. Stel n staat op positie k (met natuurlijk $k \neq n$). Waar staat k? Allereerst kan k op positie n staan, de overige getallen $1, \ldots, k-1, k+1, \ldots, n-1$ vormen een derangement van $n-2$ objecten. Als k *niet* op positie n staat, kunnen we n vergeten, het getal op positie n naar positie k verplaatsen, en vinden we een derangement van $1, \ldots, n-1$, dus $n-1$ objecten, en elk derangement is zo te maken.

Aangezien er $n-1$ mogelijkheden voor k zijn, vinden we $d(n) = (n-1)(d(n-1)+d(n-2))$, de gevraagde formule.

48b. *inductiestap.* Gebruik de formule uit **a.** voor $d(n+1)$: $d(n+1) = n \cdot d(n) + n \cdot d(n-1)$, werk naar het antwoord toe, en vul de inductieaanname in: $\cdots = (n+1)d(n) - d(n) + nd(n-1) = (n+1)d(n) - [nd(n-1) + (-1)^n] + nd(n-1) = (n+1)d(n) - (-1)^n$. Dit is wat we willen, want $-(-1)^n = (-1)^{n+1}$.

49. Voor het gemak kiezen we een naam: $K = \{\ w \cdot w^R \mid w \in \{a,b\}^*\ \}$

49a. $L \subseteq K$, met inductie naar de opbouw van L, dus voor elke $x \in L$ laten we zien dat $x \in K$.

basis. $\lambda \in L$. Klopt.

inductie. Neem aan voor $x \in L$ geldt de bewering al, dus $x \in K$. Te bewijzen dat axa in L ($bxb \in K$ gaat op dezelfde manier). Omdat $x \in K$ kunnen we schrijven $x = w \cdot w^R$, maar dan is ook axa van die vorm, $axa = a \cdot w \cdot w^R \cdot a = (aw) \cdot (aw)^R$, dus $axa \in L$.

50. Opgave van het tentamen van Maart 2004. Uitwerking beschikbaar.

51. Een 'legaal' rijtje ter lengte n ($n \geq 1$) eindigt in precies $0, 1, 2$ of 3 `B`'s, en als het rijtje op nul `B`'s eindigt is de laatste letter een `C` (omdat we slechts twee mogelijke symbolen hebben).

Als we $g_i(n)$ ($i = 0, 1, 2, 3$) gebruiken om het aantal rijtjes ter lengte n dat eindigt in exact i `B`'s aan te geven, kunnen we de volgende inductieve vergelijkingen opstellen:

. $g_0(n+1) = \sum_{k=1}^{3} g_k(n)$;
. $g_1(n+1) = g_0(n)$;
. $g_2(n+1) = g_1(n)$;
. $g_3(n+1) = g_2(n)$;

met als beginwaarden $g_0(0) = 1$; $g_1(0) = 0$; $g_2(0) = 0$; $g_3(0) = 0$.

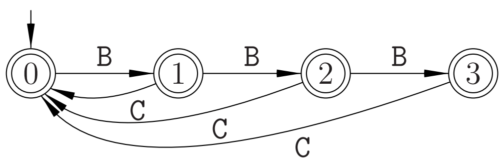
Immers, bij $g_0(n+1)$ moet de laatste letter een `C` zijn; dit zijn precies evenveel gevallen als rijtjes ter lengte n waar de laatste letter juist *geen* `C` is; daar mogen we een `C` achter plakken. Bij $g_k(n+1)$ ($k \geq 1$) tellen we rijtjes die eindigen op exact k `B`'s, dit zijn er evenveel als rijtjes ter lengte n met exact $k-1$ `B`'s aan het eind.

Het antwoord van de opgave is het getal $\sum_{k=0}^{3} g_k(N)$, de som van *alle* waarden bij gegeven N.

Voor de waarden $g_0(n)$ alleen is ook direct een inductieve vergelijking op te stellen als we bedenken dat $g_1(n) = g_0(n-1)$, $g_2(n) = g_1(n-1) = g_0(n-2)$, en ook $g_3(n) = g_0(n-3)$. Dus $g_0(n+1) = \sum_{k=1}^{3} g_0(n-k) = g_0(n-1) + g_0(n-2) + g_0(n-3)$, voor $n \geq 3$ met als beginwaarden $g_0(0) = 1, g_0(1) = 1, g_0(2) = 2, g_0(3) =$.

In het geval dat we deze reeks $g_0(n)$ weten, is het antwoord van de opgave $\sum_{k=0}^{3} g_k(N) = g_0(N) + \sum_{k=1}^{3} g_0(N-k) = \sum_{k=0}^{3} g_0(N-k)$. Kortom, we hoeven niet alle vier de reeksen te berekenen om de opgave op te kunnen lossen.

Na het lezen van het dictaat (over automaten) weten we dat er een simpele eindige automaat bij de taal van deze rijtjes hoort. De takken van de automaat 'volgen' de inductieve vergelijkingen voor $g_i(n)$ (. . . maar wat betekent dat?).



52. Dat zijn er zes, te zien in Schaum Fig.8-42, maar ook als Sloane's A000055 zie link op web-bladzijde.

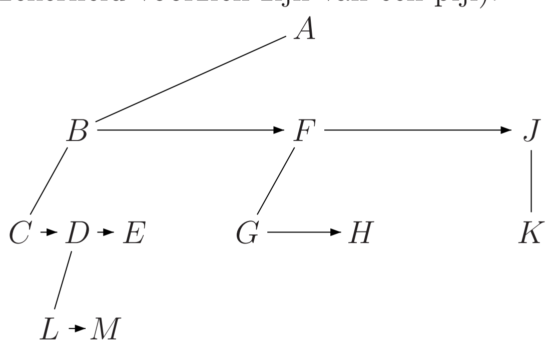
53a. Elke component is samenhangend en erft van G de eigenschap dat er geen cykels zijn, dus een boom, en geldt de relatie tussen takken en knopen (uit Theorem 8.6(ii), eigenlijk (i) $\Rightarrow$ (ii)). Voor elke component i van G afzonderlijk geldt dat $|V_i| = |E_i| + 1$, door optellen vinden we de gevraagde formule.

53b. Kortom, stel G heeft n knopen en $n-1$ takken. Dan geldt: als G zonder cykels is (ii), dan is G samenhangend (iii). oor een cykelvrije graaf geldt onze formule $|V| = |E| + c$, waarbij we reeds weten dat $|V| = n$ en $|E| = n-1$, daarom $c = 1$ dus één samenhangscomponent.

54c. postorde (via de boom bepaald)
$3x * 5z * -4 \uparrow a2b * c2 \uparrow + * /$
gehaakte infix:
$((((3*x)-(5*z)) \uparrow 4)/(a*((2*b)+(c \uparrow 2))))$.
Dit laatste kan ook door de boom te 'scannen', Schaum Fig.10-7: een interne knoop bezoeken we drie maal en schrijven bij die bezoeken achtereenvolgens een openingshaakje, het label, en een sluithaakje. Bij bladeren schrijven we bij het bezoek de label.

55c. preorde: A B C D L M E F G H J K
postorde: C L M D E B G H F J K A

55d. In de eerste-kind-rechter-broer representatie ziet boom T er als volgt uit; maw. dit is de binaire boom T', waarbij de rechter takken horizontaal getekend zijn (en voor de zekerheid voorzien zijn van een pijl).



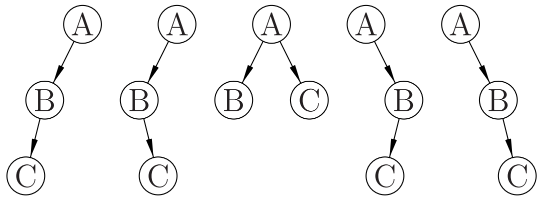
preorde: A B C D L M E F G H J K

postorde: M L E D C H G K J F B A

symmetrisch: C L M D E B G H F J K A

De preorde van beide bomen is gelijk, de symmetrische orde van deze binaire boom T' is de postorde van de originele algemene boom T.

56a. .



56b. *basis.* Voor $n = 0$ geldt $t_0 = 1$ omdat er één binaire boom is met nul knopen, de lege boom.

inductie. Kijk naar een boom met $n + 1$ knopen. Daarvan zit er één in de wortel, zitten er (zeg) k in de linker deelboom (met $0 \le k \le n$) en de overige $n - k$ in de rechter deelboom. Voor deze waarde van k kunnen we de deelbomen op t_k resp. t_{n-k} manieren kiezen, dus de hele boom heeft $t_k t_{n-k}$ mogelijkheden. Nu sommeren over alle mogelijke k.

56c. $t_0 = 1$, $t_1 = t_0 \cdot t_0 = 1 \cdot 1 = 1$, $t_2 = t_0 \cdot t_1 + t_1 \cdot t_0 = 1 \cdot 1 + 1 \cdot 1 = 2$, $t_3 = 1 \cdot 2 + 1 \cdot 1 + 2 \cdot 1 = 5$ (zie plaatje), $t_3 = 1 \cdot 5 + 1 \cdot 2 + 2 \cdot 1 + 5 \cdot 1 = 14$, $t_4 = 1 \cdot 14 + 1 \cdot 5 + 2 \cdot 2 + 5 \cdot 1 + 14 \cdot 1 = 42$, $t_5 = 1 \cdot 42 + 1 \cdot 14 + 2 \cdot 5 + 5 \cdot 2 + 14 \cdot 1 + 42 \cdot 1 = 132$, enzovoort

Deze getallen staan ook wel bekend als de getallen van Catalan, en zijn te vinden bij Slaone onder nummer A000108: 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, , … met formule $\frac{(2n)!}{n!(n+1)!}$

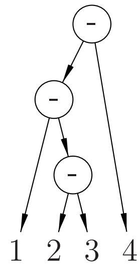
57a. Op net zoveel manieren als er bomen zijn met drie interne knopen (en vier bladeren). De structuur daarvan staat in de vorige uitwerking: maak die bomen 'vol' door alle lege kinderen door een blad te vervangen. Om er wat van op te steken zijn ook de preorde notaties gegeven.

$(((1 - 2) - 3) - 4)$	$- - -1\ 2\ 3\ 4$
$((1 - (2 - 3)) - 4)$	$- - 1 - 2\ 3\ 4$
$((1 - 2) - (3 - 4))$	$- - 1\ 2 - 3\ 4$
$(1 - ((2 - 3) - 4))$	$-1 - -2\ 3\ 4$
$(1 - (2 - (3 - 4)))$	$-1 - 2 - 3\ 4$

De boomstructuur is zichtbaar in de formule, bijvoorbeeld:

$$\overbrace{(\overbrace{(1 - (\overbrace{2 - 3}))} - 4)}$$

$$\overbrace{- \overbrace{- 1 \overbrace{- 2\ 3}}\ 4}$$



57b. 132 manieren, het 7e Catalan getal.

58. Achtereenvolgens 001, 0101, 110, 0110
Wat ontbreekt is een verklaring: waarom zit het woord niet in de taal; waarom zitten alle kortere woorden wel in de taal?

58a. Voluit: $\{1\}^* \cdot \{01\}^* \cdot \{0\}^*$.

Goed, we willen het precies weten, en schrijven alle verzamelingen uit voor strings tot-en-met lengte drie.

$\{1\}^* = \{\lambda, 1, 11, 111, \dots\}$, $\{01\}^* = \{\lambda, 01, \dots\}$, $\{0\}^* = \{\lambda, 0, 00, 000, \dots\}$,

$\{1\}^* \cdot \{01\}^* = \{\lambda, 1, 11, 111, 01, 101 \dots\} = \{\lambda, 1, 01, 11, 101, 111, \dots\}$

$\{1\}^* \cdot \{01\}^* \cdot \{0\}^* = \{\lambda, 1, 01, 11, 101, 111, 0, 10, 010, 110, 00, 100, 000, \dots\} = \{\lambda, 0, 1, 00, 01, 10, 11, 000, 010, 100, 101, 110, 111, \dots\}$.

58c. Voluit $0^*(100^*)^*1^*$.

Tot-en-met lengte drie:

$\{10\} \cdot \{0\}^* = \{10, 100, \ldots\}$.

$(\{10\} \cdot \{0\}^*)^* = \{\lambda, 10, 100, \ldots\}$. Nullen ervoor: $\{\lambda, 10, 100, 0, 00, 000, 010, \ldots\}$

Enen erachter: $\{\lambda, 10, 100, 0, 00, 000, 010, 1, 11, 111, 101, 01, 011, 001, \ldots\} =$

60a. Waar als tenminste $L \neq \varnothing$! Stel L is niet leeg, en kies een kortste woord x in L. Er is in L^2 geen woord korter dan x^2. Omdat $L = L^2$ moeten x en x^2 even lang zijn, en dus $|x| = 0$, en daarmee $x = \lambda$.

60b. Waar. Te bewijzen met inductie. *Basis:* $n = 2$: $L = L^2$ is gegeven. *Inductie:* $L^{n+1} = L^n \cdot L \stackrel{i}{=} L \cdot L \stackrel{g}{=} L$.
i: inductie-aanname; g: gegeven

60c. $L^* = \bigcup_{n \geq 0} L^n$. Hierin is $L^0 = \{ \lambda \}$ en voor $n > 0$ is $L^n = L$ vanwege het vorige onderdeel. Dus $L^* = \{ \lambda \} \cup L$. Dit is gelijk aan L omdat $\lambda \in L$ vanwege het eerste onderdeel.

Alweer is deze bewering *niet* waar voor $L = \varnothing$. Immers $\varnothing^2 = \varnothing$, terwijl $\varnothing^* = \{ \lambda \}$.

60e. Niet waar. Kies $K = \{ a \}^*$ en $L = \{ a \}$. Dan $K^* = L^*$, maar $K \not\subseteq L$.

61a. Neem $n \geq 1$. Dan $(K^*)^n = K^*$, zie Lemma **??**. Aan de andere zijde hebben we niet zo'n vereenvoudiging voor $(K^n)^*$.

Bijvoorbeeld, voor $K = \{ a \}$ en $n = 3$ $(K^*)^3 = \{ a \}^*$, terwijl $(K^3)^* = \{ aaa \}^* = \{ a^i \mid i \text{ is een drievoud} \}$.

61b. In KL zitten woorden die de concatenatie vormen van een woord uit K en een woord uit L, de volgorde is belangrijk.

Voor $K = \{ a \}$ en $L = \{ b \}$ is $KL = \{ ab \}$ en $(KL)^* = \{ \lambda, ab, abab, \ldots \}$, terwijl $LK = \{ ba \}$ en $(LK)^* = \{ \lambda, ba, baba, \ldots \}$.

61c. Er geldt dat $(K - L)M \subseteq KM - LM$, waarbij in het algemeen geen gelijkheid bestaat. Essentieel is dat sommige woorden in een concatenatie van talen op meerdere manieren kunnen ontstaan; bijvoorbeeld $a \cdot ba = ab \cdot a$. Het tegenvoorbeeld maakt daarvan gebruik: kies $K = \{ a \}$, $L = \{ ab \}$, $M = \{ a, ba \}$. dan $K - L = K$, $(K - L)M = KM = \{ aa, aba \}$, terwijl $KM - LM = \{ aa, aba \} - \{ aba, abba \} = \{ aa \}$.

62. Laat $K = \{ x \mid x \text{ bevat geen subwoord } aa \}$.

We laten met inductie naar de definitie van L zien dat $L \subseteq K$. We laten van elk woord x uit L zien dat het woord geen subwoord aa heeft.

basis. Zowel λ als a hebben geen subwoord aa.

inductiestap. Neem als *inductieaanname* dat x geen subwoord aa heeft. Daaruit volgt dat ook xb en xba geen subwoord aa heeft. Immers, de samenstellende delen x en b, ba hebben het subwoord niet, maar het kan ook niet op de grens van de concatenatie ontstaan omdat het tweede woord uit de concatenatie (b resp. ba) met een b begint.

Omgekeerd moeten we ook laten zien dat $K \subseteq L$, dwz. elk woord z zonder aa kan op de geschetste manier worden geconstrueerd.

Dit bewijzen we met inductie naar het aantal b's in z.

basis. z heeft geen b's (en x heeft ook geen subwoord aa). Dan is z gelijk aan λ of aan a. Beide woorden behoren tot L volgens (i).

inductiestap. Neem aan dat elk woord zonder aa en (maximaal) n b's tot L behoort (*inductie-aanname*).

Neem z met $n + 1$ b's en kijk naar de laatste b van z. Ofwel het is de laatste letter van $z = xb$ ofwel de een-na-laatste letter van $z =$

xba, waarin het prefix x precies n b's heeft en vanwege de aanname tot L behoort. Dan ook z omdat deze uit x geconstrueerd kan worden volgens (ii).

63a. $\{ aa, ab, ba, bb \}^*\{ a, b \}$

63b. $\{ b \}^*\{ a \}\{ b \}^*$

63c. $\{ a \}\{ a, b \}^* \cup \{ a, b \}^*\{ bb \}$

63d. $\{ a, b \}^*\{ aaa \}\{ a, b \}^*$

63e. $\{ a, b \}^*\{ bbab \}\{ a, b \}^*$

64a. Woorden met een lengte groter dan 2 kunnen alleen ontstaan door toepassing van de inductieve regel, dus door 'verdubbeling' van een woord in de taal.

0110 ontstaat uit 01 .

1010 zit niet in de taal want is niet van de vorm xx^R.

01010 zit niet in de taal want is niet van de vorm xx^R, de lengte is oneven.

Het woord 01011010 kan alleen ontstaan uit 0101 en dat woord zit niet in de taal.

64a. *basis.* Zowel 01 als 10 behoren tot K.

inductiestap. Stel x zit in L. De inductieaanname is dat x ook tot K behoort. Uit x construeren we xx^R in L. We moeten laten zien dat xx^R in K. Maar $(xx^R)^R = (x^R)^R(x)^R = xx^R$ en voldoet aan de eigenschap voor woorden uit K. We hebben de inductieaanname niet nodig.

65a. Om te kunnen redeneren met de relatie gebruiken we dat $x \mid y$ desdals er een geheel getal a is met $y = ax$.

reflexief, niet irreflexief: altijd geldt $x \mid x$ (we controleren dat 0 niet in het domein zit.)

niet symmetrisch, immers: $2 \mid 6$ terwijl $2 \nmid 6$.

asymmetrisch: stel $x \mid y$ en $y \mid x$ dan moet $x \leq y$ en ook $y \leq x$ en dus $x = y$.

transitief: stel $x \mid y$ en $y \mid z$, dan zijn er gehelen a en b met $y = ax$, $z = by$ en dus $z = (ba)x$ en daarmee is y een geheel veelvoud van x, maw. $x \mid z$.

65b. irreflexief (en niet reflexief): er geldt nooit xRx omdat $x \neq 2x$ voor $x \geq 1$.

niet transitief: $4R2$ en $2R1$ terwijl niet $4R1$.

65c.

66. Zie ook tentamen maart 2004.

67. Inderdaad, 2016 is een schrikkeljaar, net zoals 2000 dat was. We tellen de dagen beginnend met 1 januari 2000. $16 \cdot 365 + 4 + 31 + 29 \equiv 2 \cdot 1 + 4 + 3 + 1 \equiv 3 \pmod 7$.

Als 1 januari 2000 op een zaterdag (dag 1) valt, dan geeft deze berekening maandag (dag 3) aan.

68. Dit is een variant van de negenproef. Bijvoorbeeld 8123456 is deelbaar door 11 want $6 - 5 + 4 - 3 + 2 - 1 + 8 = 11$ is deelbaar.

De 'waarde' van het getal $c_k c_{k-1} \cdots c_0$ is gelijk aan $\sum_{i=0}^k c_k 10^i$. Modulo 11 geldt dat $10 \equiv -1$, $100 \equiv 1$ en inductief $10^i \equiv (-1)^i$. Daarmee $\sum_{i=0}^k c_k 10^i \equiv \sum_{i=0}^k c_k (-1)^i$. Dat is wat de opgave beweert.

69. Alle klassen ongelijk aan $\overline{0}$ zijn inverteerbaar (modulo 7). Dit volgt uit $1 \cdot 1 \equiv 1$, $2 \cdot 4 \equiv 8$, $3 \cdot 5 \equiv 15$, alles modulo 7.

Als $\overline{x}$ even is, dan is $\overline{x}$ niet inverteerbaar: immers $\overline{x} \cdot \overline{y}$ is dan altijd even (modulo 10) en niet gelijk aan $\overline{1}$. Idem voor $\overline{5}$ en vijfvouden.

De overige getallen zijn inverteerbaar: $1 \cdot 1 = 1$, $3 \cdot 7 = 21$, $9 \cdot 9 = 81$ (en dus, modulo 10, $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{3} \cdot \overline{7} = \overline{1}$, $\overline{7} \cdot \overline{3} = \overline{1}$, en $\overline{9} \cdot \overline{9} = \overline{1}$).

Dit suggereert: $\overline{x}$ is inverteerbaar modulo n precies als x en n geen delers gemeenschappelijk hebben.

70a.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

70b. Zoek de enen in de vermenigvuldigingstabel. $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{3} \cdot \overline{3} = \overline{1}$. Dus $\overline{1}$ en $\overline{3}$ zijn inverterbaar.

70c. Achtervolgens $(\overline{x}, \overline{x}^2, \overline{x}^4)$ voor alle restklassen. $(\overline{0}, \overline{0}, \overline{0})$; $(\overline{1}, \overline{1}, \overline{1})$; $(\overline{2}, \overline{0}, \overline{0})$; $(\overline{3}, \overline{1}, \overline{1})$. Waarmee de gelijkheid uit de opgave is aangetoond.

70d. $x^4 - x^2$ is deelbaar door vier, als $x^4 \equiv x^2 \pmod 4$ voor alle $x \in \mathbb{Z}$. Oftewel, voor de restklassen geldt $\overline{x^4} = \overline{x^2}$, maar dit is gelijk aan $\overline{x}^4 = \overline{x}^2$, en dat hebben we hierboven aangetoond.

Anders: $x^4 - x^2 = x^2(x-1)(x+1)$. Voor even x bevat x^2 tenminste twee factoren twee, voor oneven x bevatten zowel $x - 1$ als $x + 1$ elk een factor twee.

71a. Achtereenvolgens $(\overline{x}, \overline{x}^2, \overline{x}^3, \overline{x}^6, \overline{x}^12)$ voor alle restklassen: $(\overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1})$; $(\overline{2}, \overline{4}, \overline{8}, \overline{12}, \overline{1})$; $(\overline{3}, \overline{9}, \overline{1}, \overline{1}, \overline{1})$; $(\overline{4}, \overline{3}, \overline{12}, \overline{1}, \overline{1})$; $(\overline{5}, \overline{12}, \overline{8}, \overline{12}, \overline{1})$; $(\overline{6}, \overline{10}, \overline{8}, \overline{12}, \overline{1})$; etc. We stoppen hier.

71b. Modulo 13 geldt dus $100^{100} \equiv 100^{96} \cdot 100^4 \equiv 1 \cdot 100^4$ omdat $100^{96} = (100^{12})^8$ en elke twaalfdemacht levert 1 volgens **a**. Het grondtal mogen we daarentegen modulo 13 nemen: $100^{100} \equiv 100^4 \equiv 9^4 \equiv 81^2 \equiv 3^2 \equiv 9$.

Evenzo $1000^{1000} \equiv 1000^4 \equiv (-1)^4 \equiv 1$.

Totale rest $9 + 1 = 10$.

72a. Neem een vast geheel getal n. Dan is de verzameling $\{n\} \times \mathbb{N} = \{(n, y) \mid y \in \mathbb{N}\}$ natuurlijk aftelbaar (de bijectie met $\mathbb{N}$ is duidelijk). Maar $\mathbb{N} \times \mathbb{N} = \bigcup_{n \in \mathbb{N}} \{n\} \times \mathbb{N}$ is de aftelbare vereniging van aftelbare verzamelingen, dus aftelbaar.

We kunnen ook direct cantor-wandelen: Het paar (x, y) staat ook op die positie in een oneindig bij oneindig matrix en we kunnen een zo een opsomming bereiken: $(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (3,0), \ldots$.

72b. We kunnen de elementen van Σ^* opsommen: gesorteerd op lengte daarbinnen alfabetisch. De opsomming geeft een bijectie met $\mathbb{N}$.

72c. Deze verzameling kunnen we niet zo makkelijk opsommen als Σ^*. Er zijn oneindig veel rijtjes van lengte één. We kunnen ingewikkeld gaan Cantor-wandelen, of gewoon een resultaat toepassen.

Voor $n \in \mathbb{N}$ schrijven we V_n voor de verzameling van alle rijtjes met lengte niet langer dan n waarvan alle elementen tussen $-n$ en n inliggen. Elke V_n is eindig en $\bigcup_{n \in \mathbb{N}} V_n$ is precies de verzameling eindige rijtjes gehele getallen. Elke eindige verzameling is aftelbaar (per definitie). Vanwege Stelling **??** is deze aftelbare vereniging van aftelbare verzamelingen aftelbaar.

73a. Per definitie is A (oneindig!) aftelbaar als A gelijkmachtig is met $\mathbb{N}$ aftewel als er een bijectie is tussen A en $\mathbb{N}$. Volgens een stelling uit het dictaat mag ook genomen worden dat er een surjectieve afbeelding van $\mathbb{N}$ naar A bestaat (zogezegd een aftelling met herhalingen).

Hier gaat het over een injectieve afbeelding van A naar $\mathbb{N}$, dan krijgt elk element van A een nummer, maar gebruiken we niet alle natuurlijke getallen in de nummering. Oplossing? Hernummeren! Het element met het laagste nummer krijgt nummer 0, etc. We krijgen dan een bijectie met $\mathbb{N}$ als A tenminste oneindig is, anders is A eindig en is A per definitie aftelbaar.

73b. Voor een aftelbare verzameling V bestaat er een bijectieve afbeelding f van V naar $\mathbb{N}$. Voor $X \subseteq V$ nemen we de restrictie $f|_X$ van f tot X. Dat is een functie van X naar $\mathbb{N}$, niet meer surjectief, maar nog wel injectief. Volgens het vorige onderdeel is X aftelbaar.

Met als speciale toepassing: Σ^* is aftelbaar, dus elke taal is aftelbaar, als deelverzameling van een Σ^*.

74. Kennelijk is de bedoeling om ons daar van te overtuigen; maar hoe doen we dat? We kunnen rechtstreeks met diagonalisatie laten zien dat een taal niet aftelbaar is, of we kunnen laten zien dat de taal gelijkmachtig is met een taal waarvan we al weten dat die niet aftelbaar is; $\mathcal{P}(\mathbb{N})$ volgens het dictaat.

74a. Een functie f van $\mathbb{N}$ naar $\{0,1\}$ kan eenvoudig geïnterpreteerd worden als deelverzameling van $\mathbb{N}$: $V_f = \{n \in \mathbb{N} \mid f(n) = 1\}$, maw. f geeft enen op de plek van de getallen die in de verzameling zitten. De afbeelding $\varphi : \{0,1\}^{\mathbb{N}} \to \mathcal{P}(\mathbb{N})$ waarvoor $\varphi(f) = V_f$ is een bijectie (surjectief en injectief) en dus is $\{0,1\}^{\mathbb{N}}$ overaftelbaar (net als $\mathcal{P}(\mathbb{N})$). We hebben hier de notatie B^A gebruikt voor de verzameling van alle functies van A naar B.

74b. Een taal over dat alfabet is een deelverzameling van $\{0,1\}^*$, de verzameling van al die deelverzamelingen (talen) is dus de machtsverzameling $\mathcal{P}(\{0,1\}^*)$. Omdat $\{0,1\}^*$ aftelbaar oneindig is, is $\mathcal{P}(\{0,1\}^*)$ dat niet (omdat geen enkele verzameling gelijkmachtig is met zijn machtsverzameling).

75. (i) $\{\ w \in \{a,b\}^* \mid w$ bevat tenminste twee b's $\} = \{\ w \in \{a,b\}^* \mid \#_b(w) \geq 2\ \}$

Enerzijds heeft elk woord langs een wandeling van 0 naar 2 tenminste twee b's vanwege de takken $(0,b,1)$ en $(1,b,2)$, anderzijds heeft elk woord met tenminste twee b's een wandeling in de automaat (tot aan de eerste b in toestand 0 blijven, dan op de eerste b naar toestand 1, daar blijven en met de tweede b naar toestand 2 alwaar elk woord een wandeling heeft).

U ziet: geen gedoe met inductie, gezond verstand lijkt hier te volstaan.

Een mogelijke reguliere expressie: $a^*ba^*\{a,b\}^*$.

(ii) $\{\ w \in \{0,1\}^* \mid \#_1(w) \equiv 2 \pmod 3\ \}$

De automaat telt 1-en modulo drie. Bij 0-en wordt niet van toestand veranderd.

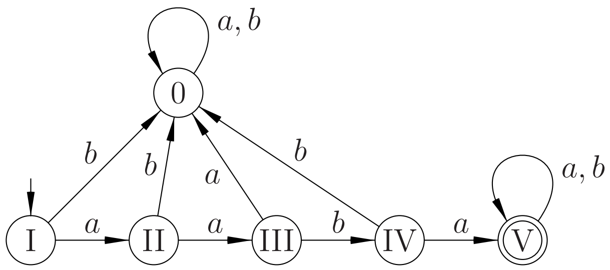
75. (iii) $\{\ w \in \{a,b\}^* \mid w$ eindigt op $aa\ \}$

De automaat houdt de laatste twee letters van de wandeling in de toestand bij. Toestanden 1, 2, en 3 komen overeen met suffix $.b$, ba en aa respectievelijk. Hieruit volgt de correctheid.

75. (v) Er is vanuit I geen tak met label b, dus $E^*(I,bx) = \varnothing$ voor elk woord x. Voor $n \geq 0$ geldt $E^*(I, b^0aabab^n) = \{\mathrm{V}\}$.

Talen van woorden leidend naar toestand I: $\{\ \lambda\ \}$ II: $\{\ a\ \}$ III: $\{\ aa\ \}$ IV: $\{\ aab\ \}$ V: $\{\ aaba\ \} \cdot \{a,b\}^*$, woorden beginnend met $aaba$.

De automaat is niet deterministisch, maar het toevoegen van een extra toestand en een aantal ontbrekende takken leidt tot een deterministische automaat zonder dat de taal verandert. Zo'n toestand, die de ontbrekende takken opvangt, heet wel een *garbage* toestand.



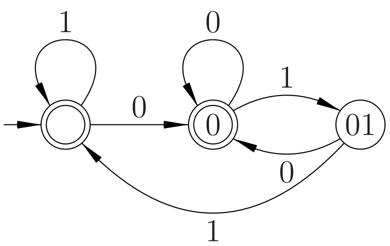
75. (vi) Elk woord heeft een wandeling van toestand I naar I, vanwege de loops. Natuurlijk maakt *aaba* weer de oversteek van I naar V. Kortom $E^*(I, b^m aabab^n) = \{\mathrm{I}, \mathrm{V}\}$, voor alle $m, n \in \mathbb{N}$.

De automaat is niet deterministisch vanwege twee uitgaande takken met label a in I. Toevoegingen helpen dus niet, een geheel nieuw ontwerp is nodig, zie onderdeel **d** hierna.

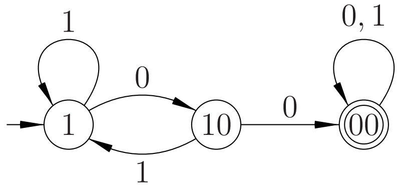
Talen van woorden leidend naar toestand I: $\{a,b\}^*$ II: $\{a,b\}^* \cdot \{\ a\ \}$, alle woorden eindigend op a III: $\{a,b\}^* \cdot \{\ aa\ \}$ IV: $\{a,b\}^* \cdot \{\ aab\ \}$ V: $\{a,b\}^* \cdot \{\ aaba\ \} \cdot \{a,b\}^*$, woorden met deelwoord *aaba*.

ps. Deze staat in de college-transparanten met $\{0, a\}$ als alfabet in plaats van $\{a, b\}$.

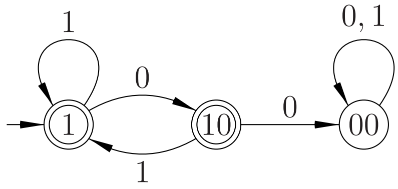
76b. We houden in de gaten hoeveel van het suffix van 01 we de laatste letters gezien hebben.



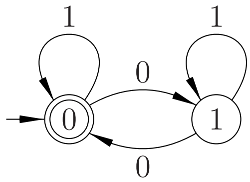
76c. Een *deterministische* automaat om juist wél het deelwoord 00 op te sporen is:



De gevraagde taal heeft precies het complement als inhoud, zie hieronder. De toestand 00 is niet essentieel voor de taal, maar wél voor determinisme!

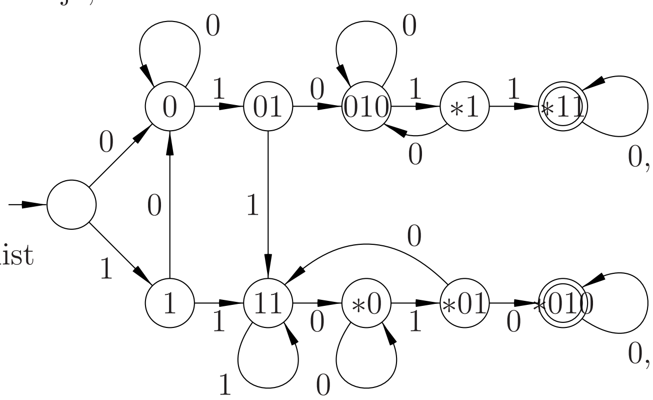


76d. Tel de voorkomens van 0 modulo twee, dus wissel tussen twee toestanden bij letter 0.



76f. Een niet-deterministische automaat heeft twee paden van begin- naar eindtoestand. Eén met label $11 \cdot 010$, en één met label $010 \cdot 11$, elk met een loop voor beide symbolen op de knoop op de plek van de punt. Ook de begin- en eindtoestand hebben twee loops.

Het construeren van een deterministische automaat lijkt me hier een heidens karwei. Nou, ja, als het moet ...



76g. Tentamen december 2004.

76h. We gebruiken drie maal de basiseenheid om 00 op te sporen.