Lusvrije ontleding van eindige automaten

Otten, R.H.J.M.

Award date:
1971

LUSVRIJE ONTLEDING VAN EINDIGE AUTOMATEN

Deel 2: Definities, stellingen en algoritmen.

Ralph Otten

0. Grondbegrippen en notaties

0.1. Junctorenlogica

0.1.1. Een bewering is waar of onwaar.

0.1.2. Conjunctie: $a \wedge b$ is een bewering die slechts dan waar is, als de beweringen a en b beide waar zijn.

0.1.3. Adjunctie: $a \vee b$ is een bewering die slechts dan onwaar is, als de beweringen a en b beide onwaar zijn.

0.1.4. Implicatie: $a \Rightarrow b$ is een bewering die slechts dan onwaar is, als de bewering a waar is en de bewering b onwaar.

0.1.5. Equivalentie: $a \Leftrightarrow b$ is een bewering die slechts dan waar is, als de beweringen a en b beide waar of beide onwaar zijn.

0.1.6. Negatie: $\neg a$ is een bewering die waar is, als a onwaar is, en die onwaar is, als a waar is.

0.1.7. 0.1.2. t/m 0.1.6. kunnen samengevat worden in waarheidstabellen:

a	$\neg a$
w	o
o	w

a	b	$a \wedge b$	$a \vee b$	$a \Rightarrow b$	$a \Leftrightarrow b$
w	w	w	w	w	w
w	o	o	w	o	o
o	w	o	w	w	o
o	o	o	o	w	w

0.2. Verzamelingen

0.2.1. $x \in V$ betekent dat x een element van de verzameling V is.
$x \notin V$ betekent dat x geen element van de verzameling V is.

0.2.2. Men kan een verzameling beschrijven door een opsomming van zijn elementen:

$$V = \{a,b,c,d,e,f,g\}$$

Natuurlijk kan dit alleen bij eindige verzamelingen.

opm: Er is geen verschil tussen de verzamelingen
$\{a,b,c,b,d,d,b,e,f,g\}$ en $\{a,e,d,c,g,f,b\}$
dwz. noch de volgorde, noch de herhalingen in de opsomming van de elementen van een verzameling zijn van belang.

0.2.3. Volzinnen die een veranderlijke bevatten en die in beweringen overgaan, als men voor zo'n veranderlijke een element uit een geschikte individuenverzameling substitueert, heten beweringsvormen of predikaten.

0.2.4. Men kan iedere verzameling beschrijven door een 'definiërende beweringsvorm' P(x):
$V = \{x|P(x)\}$ betekent dat V de verzameling is van alle x die, als ze in P(x) gesubstitueert worden, een ware bewering leveren.

0.2.5. $\emptyset$ stelt de lege verzameling voor. Deze bevat geen enkel element.

0.2.6. Een verzameling is eindig, als ze eindig veel elementen bevat. Het aantal elementen van een eindige verzameling V geven we aan met $|V|$. We noemen $|V|$ de kardinaliteit van V.
Een verzameling heet aftelbaar als haar elementen in een-eenduidige correspondentie gebracht kunnen worden met de natuurlijke getallen. Symbolisch geven we de kardinaliteit van zo'n verzameling aan met $\aleph_0$.
In alle andere gevallen heet een verzameling overaftelbaar.

0.3. Kwantorenlogica

0.3.1. Voor een variabele waarvoor men iets kan invullen, heeft men de naam vrije variabele gekozen. Is substitutie niet mogelijk, dan heet de veranderlijke gebonden. Men kan veranderlijke binden door zgn. kwantoren.

0.3.2. Universele kwantor: $\forall_{x\in V}[P(x)] \Leftrightarrow (x \in V \Rightarrow P(x))$

0.3.3. Existentiële kwantor: $\exists_{x\in V}[P(x)] \Leftrightarrow (\{x \mid (x \in V) \wedge P(x)\} \neq \emptyset)$

0.3.4. Enkele regels uit de kwantorenlogica:

a. $\forall_{x\in V} \forall_{y\in W}[P(x,y)] \Leftrightarrow \forall_{y\in W} \forall_{x\in V}[P(x,y)]$

b. $\exists_{x\in V} \exists_{y\in W}[P(x,y)] \Leftrightarrow \exists_{y\in W} \exists_{x\in V}[P(x,y)]$.

c. $(a \wedge \exists_{x\in V}[P(x)]) \Leftrightarrow \exists_{x\in V}[a \wedge P(x)]$ mits de variabele x in de bewering a niet vrij voorkomt.

d. $\forall_{x\in V}[P(x) \Rightarrow a] \Leftrightarrow \exists_{x\in V}[P(x)] \Rightarrow a$

opm: de regel $\forall_{x\in V} \exists_{y\in W}[P(x,y)] \Leftrightarrow \exists_{y\in W} \forall_{x\in V}[P(x,y)]$ is niet correct!

0.3.5. $\exists!_{x\in V}[P(x)] \Leftrightarrow \exists_{x\in V}[P(x) \wedge (\forall_{y\in V}[P(y) \Rightarrow (x=y)])]$

0.4. Families

0.4.1. Een familie onderscheidt zich van een verzameling doordat herhalingen van elementen nu wel belangrijk zijn. Zo geldt voor families:
$\{a,b,b,b,c,e,f,g\} = \{a,b,c,b,f,g,e,b\} \neq \{a,e,f,c,g,b\}$
Volgorde in de opsomming is dus weer niet belangrijk!
Soms worden gelijke elementen in een familie van elkaar onderscheiden door indices; dan kan men de familie als een verzameling zien.

0.4.2. De som van twee families A en B, aangegeven door $A \dot{+} B$, is de familie bestaande uit alle elementen (inclusief herhalingen) van A en B. Het aantal elementen van $A \dot{+} B$ is dus de som van het aantal elementen van A en B afzonderlijk:
$\{a,a,b,b,b,c,d\} \dot{+} \{a,b,b,c,e,e\} = \{a,a,a,b,b,b,b,b,c,c,d,e,e\}$

0.4.3. Het verschil $A \dot{-} B$ van twee families is alleen gedefinieerd als alle elementen van B minstens evenveel keren in A voorkomen. $A \dot{-} B$ bestaat dan uit die elementen van A die overblijven, nadat men de familie B uit A verwijderd heeft:
$\{a,a,b,b,b,c,d\} \dot{-} \{a,b,b,c\} = \{a,b,d\}$

1. Verzamelingen

1.1. Verzamelingen

1.1.1. W heet een deelverzameling van de verzameling V, (notatie: $W \subseteq V$) als voor alle x uit de bewering $x \in W$ de bewering $x \in V$ volgt:

$\forall_{x \in W} [x \in V] \Leftrightarrow W \subseteq V$
$\emptyset \subseteq A$
$A \subseteq A$
$A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$
$A \subset B \Leftrightarrow (A \subseteq B) \wedge (\neg(A = B))$
De deelverzamelingen van een verzameling V zijn de elementen van de machtsverzameling PV van V.

1.1.2. De doorsnede $A \cap B$ van twee verzamelingen A en B gedefinieerd door
$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$
kan ook gedefinieerd worden door
$x \in A \cap B \Leftrightarrow (x \in A) \wedge (x \in B)$

1.1.3. De vereniging van twee verzamelingen A en B wordt gedefinieerd door
$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$
oftewel
$x \in A \cup B \Leftrightarrow (x \in A) \vee (x \in B)$

1.1.4. De definitie van de doorsnede van willekeurig veel verzamelingen luidt:
Zij Q een deelverzameling van PV, dan
$\bigcap_{X \in Q} X = \bigcap_{Q} X = \{a \mid \forall_{X \in Q} [a \in X]\}$ oftewel $a \in \bigcap_{X \in Q} X \Leftrightarrow \forall_{X \in Q} [a \in X]$

1.1.5. De vereniging van willekeurig veel verzamelingen noteert men als volgt:
Zij Q een deelverzameling van PV, dan
$\bigcup_{X \in Q} X = \bigcup_{Q} X = \{a \mid \exists_{X \in Q} [a \in X]\}$ oftewel $a \in \bigcup_{Q} X \Leftrightarrow \exists_{X \in Q} [a \in X]$

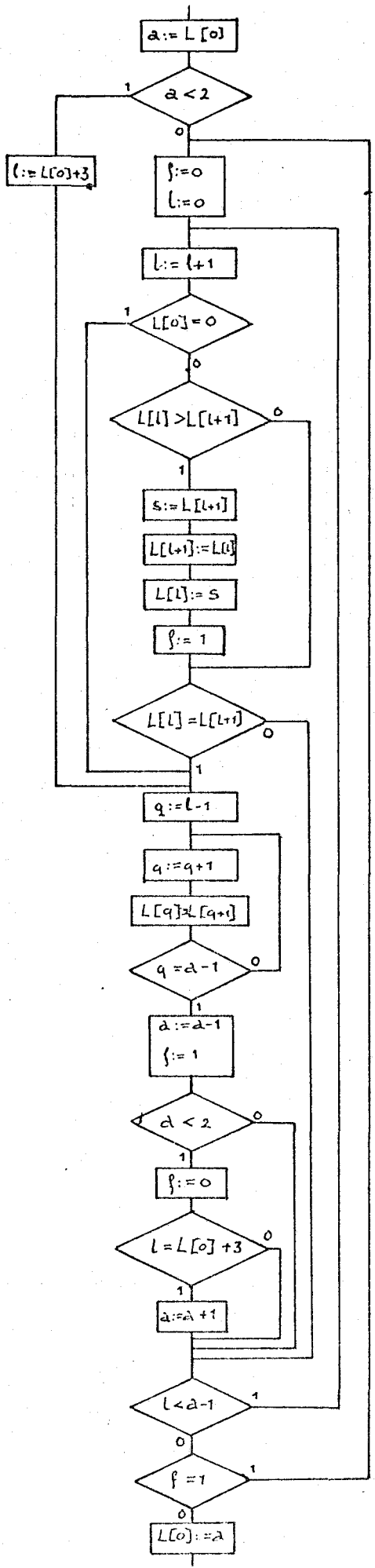
1.1.6. Het verschil $A \backslash B$ van twee verzamelingen A en B wordt gedefinieerd door:
$A \backslash B = \{x \mid (x \in A) \wedge (x \notin B)\}$ oftewel $x \in A \backslash B \Leftrightarrow (x \in A) \wedge (x \notin B)$

1.1.7. Voor de regels die gelden voor de verzamelingtheoretische bewerkingen hierboven gedefinieerd, verwijs ik naar de boeken op het gebied van de verzamelingenleer.

1.1.8. Onder het cartesisch produkt van de verzamelingen $V_1, V_2, \ldots, V_k$ wordt verstaan:
$V_1 \times V_2 \times V_3 \ldots \times V_k = \{(x_1, x_2, x_3 \ldots, x_k) \mid \forall_{1 \leq i \leq k} [x_i \in V_i]\}$

1.2. Het algoritme LEX

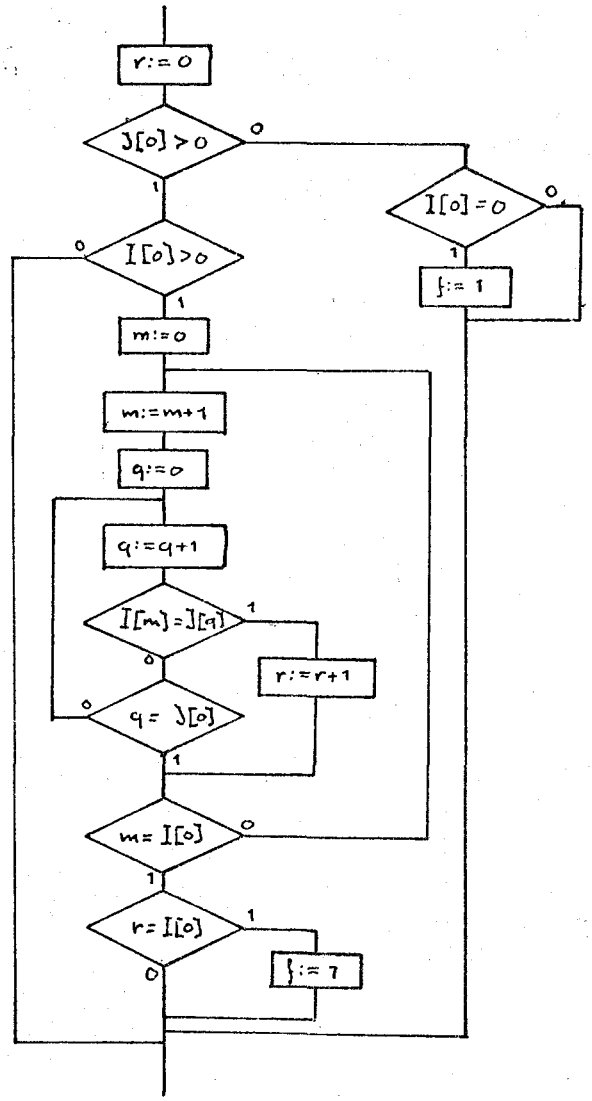
We hebben een familie L waarvan de elementen niet-negatieve getallen zijn.
Het algoritme LEX zet alle elementen van L in natuurlijke volgorde, zorgt dat elk element slechts eenmaal genoemd wordt en verwijdert het getal 0 (indien aanwezig).
Bij 'begin' geldt: L[0]= aantal elementen van de familie L
L[1] t/m L[L[0]] = elementen van de familie L
Bij 'einde' geldt: L[0]= aantal elementen van de gevormde verzameling
L[1] t/m L[L[0]] = elementen van de verzameling


a := L[0]
a < 2
1
0
l := L[0]+3
f := 0
l := 0
l := l+1
L[0] = 0
1
0
L[l] > L[l+1]
0
1
s := L[l+1]
L[l+1] := L[l]
L[l] := s
f := 1
L[l] = L[l+1]
0
1
q := l-1
q := q+1
L[q] := L[q+1]
q = a-1
0
1
a := a-1
f := 1
a < 2
0
1
f := 0
l = L[0] +3
0
1
a := a +1
l < a-1
1
0
f = 1
1
0
L[0] := a

1.3. Het algoritme INCL

We hebben twee verzamelingen, I en J, waarvan de elementen positieve getallen zijn.
I[0]=|I|
I[1] t/m I[I[0]] zijn de elementen van I
J[0]=|J|
J[1] t/m J[J[0]] zijn de elementen van J

Bij 'einde' geldt: f=1 als $I \subseteq J$
f=0 als $I \not\subseteq J$



2. Relaties en relationaalstructuren

2.1. Relaties

2.1.1. Een beweringsvorm $P(x_1, x_2, \ldots, x_k)$ met $x_i \in V_i$ voor $1 \leq i \leq k$ definieert een deelverzameling R_P van $V_1 \times V_2 \ldots \times V_k$:
$R_P = \{(x_1, x_2, \ldots, x_k) \mid P(x_1, x_2, \ldots, x_k)\}$
oftewel
$(x_1, x_2, \ldots, x_k) \in R_P \Leftrightarrow P(x_1, x_2, \ldots, x_k)$
R_P heet de door P gedefinieerde k-aire relatie.

2.1.2. Daar iedere verzameling door een beweringsvorm gedefinieerd kan worden (0.2.4.) is iedere deelverzameling van $V_1 \times V_2 \ldots \times V_k$ een k-aire relatie.

2.1.3. $R_{P_1} \subseteq R_{P_2} \Leftrightarrow \forall_{x_1 \in V_1} \forall_{x_2 \in V_2} \ldots\ldots\ldots \forall_{x_k \in V_k} [P_1(x_1, x_2, \ldots, x_k) \Rightarrow P_2(x_1, x_2, \ldots, x_k)]$
$R_{P_1} = R_{P_2} \Leftrightarrow \forall_{x_1 \in V_1} \forall_{x_2 \in V_2} \ldots\ldots\ldots \forall_{x_k \in V_k} [P_1(x_1, x_2, \ldots, x_k) \Leftrightarrow P_2(x_1, x_2, \ldots, x_k)]$

2.1.4. Een relatie R_P heet rechtseenduidig als
$\forall_{x_1 \in V_1} \forall_{x_2 \in V_2} \ldots\ldots\ldots \forall_{u \in V_k} \forall_{v \in V_k} [P(x_1, x_2, \ldots, u) \wedge P(x_1, x_2, \ldots, v) \Rightarrow u = v]$
Zo'n relatie heet een afbeelding uit $V_1 \times V_2 \ldots \times V_{k-1}$ in V_k.
$(x_1, x_2, \ldots, x_{k-1})$ heet het argument, u het beeld van R_P.

2.1.5. Een relatie heet linkstotaal als
$\forall_{x_1 \in V_1} \forall_{x_2 \in V_2} \ldots\ldots\ldots\ldots \exists_{x_k \in V_k} [(x_1, x_2, \ldots, x_k) \in R_P]$
Zo'n relatie heet een afbeelding van $V_1 \times V_2 \ldots \times V_{k-1}$ in V_k, als zij ook rechtseenduidig is.

2.1.6. Een afbeelding van $V_1 \times V_2 \ldots \times V_{k-1}$ in V_k heet injectief of een-eenduidig als
$\forall_{x_1 \in V_1} \ldots \forall_{x_{k-1} \in V_{k-1}} \forall_{y_1 \in V_1} \ldots \forall_{y_{k-1} \in V_{k-1}} \forall_{x \in V_k} [P(x_1, x_2, \ldots, x) \wedge P(y_1, y_2, \ldots, x) \Rightarrow (x_1 = y_1) \wedge (x_2 = y_2) \wedge \ldots \wedge (x_{k-1} = y_{k-1})]$
dwz. R_P is linkseenduidig.

2.1.7. Een afbeelding van $V_1 \times V_2 \ldots \times V_{k-1}$ in V_k heet surjectief als
$\forall_{x_k \in V_k} \exists_{x_1 \in V_1} \exists_{x_2 \in V_2} \ldots \exists_{x_{k-1} \in V_{k-1}} [P(x_1, x_2, \ldots, x_k)]$
dwz. R_P is rechtstotaal.
Zo'n relatie heet een afbeelding van $V_1 \times V_2 \ldots \times V_{k-1}$ op V_k.

2.1.8. Een afbeelding die zowel injectief als surjectief is, heet bijectief.

2.2. Binaire relaties

2.2.1. Een deelverzameling van VxW heet een binaire relatie.
Als R een binaire relatie is en $(x,y) \in R$, dan schrijven we vaak xRy.

2.2.2. Speciale binaire relaties zijn:
de zgn. alrelatie: $xUy \Leftrightarrow (x,y) \in V \times W$,
de zgn. nulrelatie: $x\emptyset y = \emptyset$.
We spreken over een 'relatie over V' als R een deelverzameling van VxV is.
$xD_V y \Leftrightarrow x = y$

2.2.3. De inverse R^{-1} van een binaire relatie $R \subseteq V \times W$ wordt gedefinieerd door:
$\forall_{x \in W} \forall_{y \in V} [xR^{-1}y \Leftrightarrow yRx]$

2.2.4. Het domein van de binaire relatie $R \subseteq V \times W$ is de verzameling:
$pr_1 R = \{v \mid \exists_{w \in W} [vRw]\}$
Het bereik van de binaire relatie $R \subseteq V \times W$ is de verzameling:
$pr_2 R = \{w \mid \exists_{v \in V} [vRw]\} = pr_1 R^{-1}$
$pr_1 R \subseteq V$
$pr_2 R \subseteq W$

2.2.5. De binaire relatie $\varphi \subseteq V \times W$ is een afbeelding uit V in W slals
$\forall_{v \in V} [(v \varphi w_1 \wedge v \varphi w_2) \Rightarrow w_1 = w_2]$
φ is een afbeelding van V in W slals $pr_1 \varphi = V$ en φ is rechtseenduidig
φ is een afbeelding van V op W slals $pr_1 \varphi = V$ en $pr_2 \varphi = W$ en φ is rechtseenduidig.

2.2.6. $v\varphi$ = het beeld van v onder de afbeelding φ (ook wel $\varphi(v)$)
$vR = \{w \mid vRw\}$
Voor $V' \subseteq V$: $V'R = \bigcup_{v \in V'} vR$

2.2.7. φ^{-1} is een afbeelding slals φ een-eenduidig is.
Als $\varphi \subseteq V \times V$ en φ is een een-eenduidige afbeelding, dan heet φ een permutatie.
Als φ een permutatie is, dan is φ^{-1} het ook.

2.3. Produkt van binaire relaties

2.3.1. $R \subseteq V_1 \times V_2$ en $S \subseteq V_2 \times V_3$.
De door
$xRSy \Leftrightarrow \exists_{z \in V_2} [xRz \wedge zSy]$
gedefinieerde relatie $RS \subseteq V_1 \times V_3$ heet het produkt van de relaties R en S.

2.3.2. $R \subseteq V_1 \times V_2$, $S \subseteq V_2 \times V_3$ en $T \subseteq V_3 \times V_4$
Produktvorming heeft de associatieve eigenschap, dwz. $(RS)T = R(ST)$

bewijs: $x(RS)Ty \Leftrightarrow \exists_{w \in V_3} [\exists_{z \in V_2} [(xRz) \wedge (zSw)] \wedge wTy]$
$xR(ST)y \Leftrightarrow \exists_{z \in V_2} [(xRz) \wedge \exists_{w \in V_3} [(zSw) \wedge (wTy)]]$
volgens 0.3.4.b en c : $x(RS)Ty \Leftrightarrow xR(ST)y$

2.3.3. $R \subseteq V_1 \times V_2$ en $S \subseteq V_1 \times V_2$.
$D_{V_1} R = R D_{V_2} = R$
$D_V = D_V^{-1}$
$(R^{-1})^{-1} = R$
$RS = \emptyset \Leftrightarrow (pr_2 R \cap pr_1 S = \emptyset)$
$(RS)^{-1} = S^{-1} R^{-1}$
$R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$
Als R en S rechtseenduidig zijn, dan is RS het ook.
Als R en S linkstotaal zijn, dan is RS ook linkstotaal.
Als R en S afbeeldingen zijn, dan is RS dus ook een afbeelding.

2.3.4. $R_1 \subseteq S_1 \wedge R_2 \subseteq S_2 \Rightarrow R_1 R_2 \subseteq S_1 S_2$

bewijs: $xR_1R_2y \Leftrightarrow \exists_z [xR_1z \wedge zR_2y]$
$R_1 \subseteq S_1 \Rightarrow xR_1z \wedge xS_1z$
$R_2 \subseteq S_2 \Rightarrow zR_2y \wedge zS_2y$
$\Big\} xR_1R_2y \Rightarrow \exists_z [xS_1z \wedge zS_2y]$ dwz. xS_1S_2y.

2.3.5. φ is een afbeelding van A in B.
$D_A \subseteq \varphi\varphi^{-1}$
$D_{pr_2\varphi} = \varphi^{-1}\varphi$

bewijs: $x\varphi^{-1}\varphi y \Leftrightarrow \exists_{z \in A} [x\varphi^{-1}z \wedge z\varphi y] \Leftrightarrow \exists_{z \in A} [z\varphi x \wedge z\varphi^{-1}y] \Rightarrow x=y$ voor alle $x \in pr_2\varphi$.

$x\varphi\varphi^{-1}y \Leftrightarrow \exists_{z \in B} [x\varphi z \wedge z\varphi^{-1}y] \Leftrightarrow \exists_{z \in B} [x\varphi z \wedge y\varphi z]$ en dit geldt in ieder geval voor $y=x$.

2.4. Eigenschappen van binaire relaties

2.4.1. $R \subseteq V \times W$
$R^{-1}R \subseteq D_W \Rightarrow$ R is rechtseenduidig.

bewijs: $R^{-1}R \subseteq D_W$ betekent: $\forall_{y\in W} \forall_{z\in W} [yR^{-1}Rz \Rightarrow y=z]$
$\forall_{y\in W} \forall_{z\in W} [\exists_{x\in V} [(yR^{-1}x) \wedge (xRz)] \Rightarrow y=z]$
$\forall_{y\in W} \forall_{z\in W} [\forall_{x\in V} [(xRy) \wedge (xRz) \Rightarrow y=z]]$
$\forall_{y\in W} \forall_{z\in W} \forall_{x\in V} [(xRy) \wedge (xRz) \Rightarrow y=z]$
Bij dit bewijs werd gebruik gemaakt van 2.1.3.,2.3.1.,2.2.3., en 0.3.4.

2.4.2. $R \subseteq V \times W$
R is linkseenduidig als R^{-1} rechtseenduidig, dwz. $RR^{-1} \subseteq D_V$

bewijs: zie 2.4.1.

2.4.3. $R \subseteq V \times W$
$D_V \subseteq RR^{-1} \Rightarrow$ R is linkstotaal

bewijs: $D_V \subseteq RR^{-1}$ betekent $\forall_{x\in V} \forall_{y\in V} [x=y \Rightarrow \exists_{z\in W} [(xRz) \wedge (zR^{-1}y)]]$
$\forall_{x\in V} \exists_{z\in W} [(xRz) \wedge (zR^{-1}x)]$
$\forall_{x\in V} \exists_{z\in W} [xRz]$

2.4.4. $R \subseteq V \times W$
R is rechtstotaal als R^{-1} linkstotaal is, dwz. $D_W \subseteq R^{-1}R$

2.4.5. $R \subseteq V \times W$
$R^{-1}R \subseteq D_W \wedge D_V \subseteq RR^{-1} \Rightarrow$ R is een afbeelding van V in W.

2.4.6. $R \subseteq V \times W$
$RR^{-1} = D_V \wedge R^{-1}R = D_W \Rightarrow$ R is bijectief en R^{-1} is de inverse afbeelding.

2.4.7. $R \subseteq V \times V$
R heet reflexief als $\forall_{x\in V} [xRx]$
R heet antireflexief als $\forall_{x\in V} [\neg(xRx)]$

2.4.8. $R \subseteq V \times V$ en $S \subseteq V \times V$
R is reflexief $\Leftrightarrow D_V \subseteq R$
R is reflexief $\Leftrightarrow D_V \subseteq R \subseteq RR(=R^2) \subseteq RRR(=R^3) \subseteq \ldots\ldots$
R is reflexief $\Leftrightarrow R^{-1}$ is reflexief
R is reflexief $\Leftrightarrow \forall_S [RS \supseteq S]$
R is reflexief $\Rightarrow$ R is links- en rechtstotaal
R en S reflexief $\Rightarrow$ RS is reflexief

2.4.9. R heet symmetrisch als $\forall_{x\in V} \forall_{y\in V} [xRy \Rightarrow yRx]$ $(R \subseteq V \times V)$
R heet antisymmetrisch als $\forall_{x\in V} \forall_{y\in V} [(xRy) \wedge (yRx) \Rightarrow x=y]$ $(R \subseteq V \times V)$

2.4.10. $R \subseteq V \times V$
R is symmetrisch $\Leftrightarrow R=R^{-1}$
R is symmetrisch $\Leftrightarrow R^{-1}$ is symmetrisch
R is antisymmetrisch $\Leftrightarrow R \cap R^{-1} = D_V$

opm: Uit R en S symmetrisch volgt niet, dat RS symmetrisch is!

2.4.11. $R \subseteq V \times V$
R heet transitief als $\forall_{x\in V}\forall_{y\in V}\forall_{z\in V}[(xRy)\wedge(yRz)\Rightarrow(xRz)]$

2.4.12. $R \subseteq V \times V$
R is transitief $\Leftrightarrow R \subseteq R^2$
R is transitief $\Leftrightarrow R \subseteq R^2 \subseteq R^3 \subseteq \ldots\ldots$

2.4.13. $R \subseteq V \times V$
R heet rechtscomparatief als $\forall_{x\in V}\forall_{y\in V}\forall_{z\in V}[(xRy)\wedge(zRy)\Rightarrow(xRz)]$
R heet linkscomparatief als $\forall_{x\in V}\forall_{y\in V}\forall_{z\in V}[(yRx)\wedge(yRz)\Rightarrow(xRz)]$
R heet cyclisch als $\forall_{x\in V}\forall_{y\in V}\forall_{z\in V}[(yRx)\wedge(zRy)\Rightarrow(xRz)]$

2.4.14. $R \subseteq V \times V$
R is rechtscomparatief $\Leftrightarrow RR^{-1} \subseteq R$
R is linkscomparatief $\Leftrightarrow R^{-1}R \subseteq R$
R is cyclisch $\Leftrightarrow R^{-1}R^{-1} \subseteq R$

bewijs:

$$\forall_{x\in V}\ \forall_{y\in V}\ \forall_{z\in V}[(xRy)\wedge(zRy)\Rightarrow(xRz)] \Leftrightarrow$$
$$\Leftrightarrow \forall_{x\in V}\ \forall_{y\in V}\ \forall_{z\in V}[(xRy)\wedge(yRz)\Rightarrow(xRz)] \Leftrightarrow$$
$$\Leftrightarrow \forall_{x\in V}\ \forall_{z\in V}[xRR^{-1}z \Rightarrow xRz] \Leftrightarrow RR^{-1} \subseteq R$$

De andere bewijzen gaan analoog.

2.4.15. $R \subseteq V \times V$
R is rechtscomparatief en linkstotaal slals R reflexief, symmetrisch en transitief is.

bewijs: $\left.\begin{array}{l} R \text{ is linkstotaal} \Leftrightarrow D_V \subseteq RR^{-1} \\ R \text{ is rechtscomparatief} \Leftrightarrow RR^{-1} \subseteq R \end{array}\right\} \Rightarrow D_V \subseteq RR \subseteq R \Rightarrow D_V \subseteq R \Leftrightarrow R \text{ is reflexief.}$

$$\left.\begin{array}{l} D_V \subseteq R \Rightarrow D_V R^{-1} \subseteq RR^{-1} \Rightarrow R^{-1} \subseteq RR^{-1} \\ \qquad\qquad\qquad\qquad\quad RR^{-1} \subseteq R \end{array}\right\} \Rightarrow R^{-1} \subseteq R$$

$$\left.\begin{array}{l} D_V \subseteq R \Rightarrow D_V \subseteq R^{-1} \\ RR^{-1} \subseteq R \Rightarrow (RR^{-1})^{-1} = R^{-1}R \subseteq R^{-1} \end{array}\right\} \Rightarrow R = D_V R \subseteq R^{-1}R = (RR^{-1})^{-1} \subseteq R^{-1} \Rightarrow R \subseteq R^{-1}$$

$$\left.\begin{array}{l} R^{-1} \subseteq R \\ R^{-1} = R \end{array}\right\} \Rightarrow R^2 \subseteq R \Leftrightarrow R \text{ is transitief.}$$

$$\left.\begin{array}{l} R \text{ is reflexief} \Leftrightarrow D_V \subseteq R \Rightarrow D_V \subseteq R^2 \\ R \text{ is symmetrisch} \Leftrightarrow R = R^{-1} \Rightarrow R^2 = RR^{-1} \end{array}\right\} \Rightarrow D_V \subseteq RR^{-1} \Leftrightarrow R \text{ is linkstotaal}$$

$$\left.\begin{array}{l} R \text{ is symmetrisch} \Leftrightarrow R = R^{-1} \Rightarrow R^2 = RR^{-1} \\ R \text{ is transitief} \Leftrightarrow R^2 \subseteq R \end{array}\right\} RR^{-1} \subseteq R \Leftrightarrow R \text{ is rechtscomparatief.}$$

2.4.16. Relaties over V die rechtscomparatief en linkstotaal zijn, noemen we equivalentierelaties.

2.4.17. $R \subseteq V \times V$
R is een equivalentierelatie slals R reflexief, symmetrisch en transitief is.

bewijs: 2.4.15 en 2.4.16.

2.5. Relationaalstructuren

2.5.1. Een verzameling waarop een systeem van relaties gedefinieerd is, heet een relationaalstructuur.

2.5.2. $(V; R_1, R_2, \ldots, R_k)$ en $(V'; R_1', R_2', \ldots, R_k')$ zijn twee relationaalstructuren.
Ψ is een afbeelding die aan elke R_i precies één $R_j' = \Psi(R_i)$ toevoegt en en aan elke R_j' precies één $R_i = \Psi^{-1}(R_j')$, terwijl bovendien ΨR_i precies evenveel variabelen bevat als R_i.
φ is een afbeelding zodat
$\forall_{1\le i\le k} \; \forall_{x_1\in V} \forall_{x_2\in V} \ldots\ldots \forall_{x_n\in V}\left[(x_1, x_2, \ldots, x_n)\in R_i \Rightarrow (x_1\varphi, x_2\varphi, \ldots, x_n\varphi)\in \Psi(R_i)\right]$
Het paar (Ψ, φ) heet dan een homomorfisme.
Als $V\varphi\subseteq V$ en $\Psi R_i = R_i$, dan heet het homomorfisme een endomorfisme.
(Ψ, φ) heet een isomorfisme als (Ψ, φ) bijectief is en (Ψ', φ') een homomorfisme is.
Een endomorfisme dat tevens een isomorfisme is, heet een automorfisme.

2.5.3. Een produktoperatie $R \subseteq VxVxV$ is een afbeelding van VxV in V.
Vaak noteren we $(x,y,z)\in R$ als $R(x,y)=z$ of ook wel als $x*y=z$, waarbij $*$ een symbool voor de operatie is.

2.5.4. $(V,*)$ is een relationaalstructuur met een produktoperatie, aangegeven door $*$.
$(V,*)$ heet dan een groepoïde.
Een afbeelding φ van V in V' heet dan een homomorfisme als
$$(x*y)\varphi = x\varphi *' y\varphi$$
$(V',*')$ heet dan een homomorf beeld van $(V,*)$

2.5.5. Een equivalentierelatie S heet verenigbaar met een afbeelding R als
$\forall_{1\le i\le k-1}\left[(x_i S y_i)\right] \wedge (x_1, x_2, \ldots, x_k)\in R \wedge (y_1, y_2, \ldots, y_k)\in R \Rightarrow x_k S y_k$

Voor een produktoperatie wordt dit: $(x_1 S y_1)\wedge(x_2 S y_2)\Rightarrow (x_1 * x_2) S (y_1 * y_2)$

2.5.6. $(V; R_1, R_2, \ldots, R_k)$ is een relationaalstructuur, waarvan elke R_i een afbeelding van VxVx ... xV in V is. De equivalentierelatie S is met alle R_i verenigbaar.
S heet dan een congruentierelatie over de structuur.

Voor produktoperaties onderscheiden we nog links- en rechtscongruent:
Een equivalentierelatie S heet linkscongruent als
$\forall_{z\in V}\left[\, xSy \Rightarrow (x*z)S(y*z)\right]$
Een equivalentierelatie S heet rechtscongruent als
$\forall_{z\in V}\left[\, xSy \Rightarrow (z*x)S(z*y)\right]$

2.5.7. Een equivalentierelatie S over een groepoïde $(V,*)$, die zowel links- als rechtscongruent is, is een congruentierelatie over $(V,*)$

bewijs: $\left.\begin{array}{l} x_1 S y_1 \Rightarrow (x_1*x_2)S(y_1*x_2) \\ x_2 S y_1 \Rightarrow (y_1*x_2)S(y_1*y_2)\end{array}\right\} \Rightarrow (x_1*x_2)S(y_1*y_2)$ immers S is transitief.

2.5.8. Een produktoperatie heet commutatief als
$\forall_{x\in V}\ \forall_{y\in V}\ [\, x*y=y*x\,]$

2.5.9. Een produktoperatie heet associatief als
$\forall_{x\in V}\ \forall_{y\in V}\ \forall_{z\in V}\ [\,(x*y)*z=x*(y*z)\,]$

2.5.10. Als de produktoperatie * associatief is, dan
$\forall_{v_q\in V}\quad (v_1*v_2*\ \dots\ *v_i)*(v_{i+1}*\ \dots\ *v_n)=(v_1*v_2*\ \dots\ *v_j)*(v_{j+1}*\ \dots\ *v_n)$

bewijs: Voor $n=3$ is de stelling zeker juist. Stel nu $n>3$ en $i<j$.
We gebruiken volledige inductie:
De stelling is waar voor alle aantallen factoren $< n$.

$$(v_1*v_2*\ \dots\ *v_i)*(v_{i+1}*\ \dots\ *v_n)=(v_1*\ \dots\ *v_i)*\big((v_{i+1}*\ \dots\ *v_j)*(v_{j+1}*\ \dots\ *v_n)\big)$$
$$(v_1*v_2*\ \dots\ *v_j)*(v_{j+1}*\ \dots\ *v_n)=\big((v_1*\ \dots\ *v_i)*(v_{i+1}*\ \dots\ *v_j)\big)*(v_{j+1}*\ \dots\ *v_n)$$

Op grond van de associatieve eigenschap van * zijn de rechterleden gelijk en dus ook de linkerleden.

3. Overdekkingen

3.1. Definities

In deze paragraaf is V een eindige, niet-lege verzameling

3.1.1. De familie C heet een overdekking van V als voor elk element van C geldt dat het een deelverzameling van V is, en als de vereniging van alle elementen van C gelijk aan V is.
De elementen van C heten blokken.
Met #C geven we het grootste getal van de verzameling $\{|B| \mid B \in C\}$ aan.

3.1.2. $\mu \subseteq PV$
μ heet een verzamelingensysteem van V als μ een overdekking van V is en
$\forall_{B\in\mu}\ \forall_{B'\in\mu}\ [B \subseteq B' \Rightarrow B=B']$

3.1.3. $\mu \subseteq PV$
μ heet een partitie van V als μ een verzamelingensysteem van V is en
$\forall_{B\in\mu}\ \forall_{B'\in\mu}\ [B \neq B' \Rightarrow B \cap B' = \emptyset]$

3.1.4. μ en μ' zijn verzamelingensystemen van V .
$\mu \leq \mu' \Leftrightarrow \forall_{B\in\mu}\ \exists_{B'\in\mu'}[B \subseteq B']$
In zo'n geval heet μ fijner als μ' en μ' groffer als μ.
μ heet echt fijner als : $\mu < \mu \Leftrightarrow \forall_{B\in\mu}\ \exists_{B'\in\mu'}[B \subset B']$

3.1.5. $\mu_0, \mu_1, \mu_2, \ldots$ is een oneindige rij partities van V, zodat voor alle positieve, gehele getallen k geldt: $(\mu_{k+1} \leq \mu_k) \wedge (\mu_{k+1} = \mu_k \Rightarrow \mu_{k+2} = \mu_{k+1})$

Er is een geheel getal $K < |V|$, zodat $\mu_k = \mu_K$ voor alle $k \geq K$

bewijs: Als $\mu_{k+1} < \mu_k$ dan $|\mu_k| < |\mu_{k+1}|$
Daar $|\mu_k| \leq |V|$ kan dit slechts eindig veel keren voorkomen.
We kiezen K zodanig, dat voor k=K voor het eerst $\mu_{k+1} = \mu_k$. $K < |V|$ moet dan gelden.

3.1.6. C is een overdekking van V met als blokken $B_1, B_2, \ldots, B_n$.
$J_1 = \{1\}$
Voor $2 \leq i \leq n$: $K_i := \{i \mid \exists_{j\in J_{i-1}}[B_i \subseteq B_j]\} \cup \{j \mid j \in J_{i-1} \wedge B_j \subset B_i\}$

$J_i := (J_{i-1} \cup \{i\}) \setminus K_i$

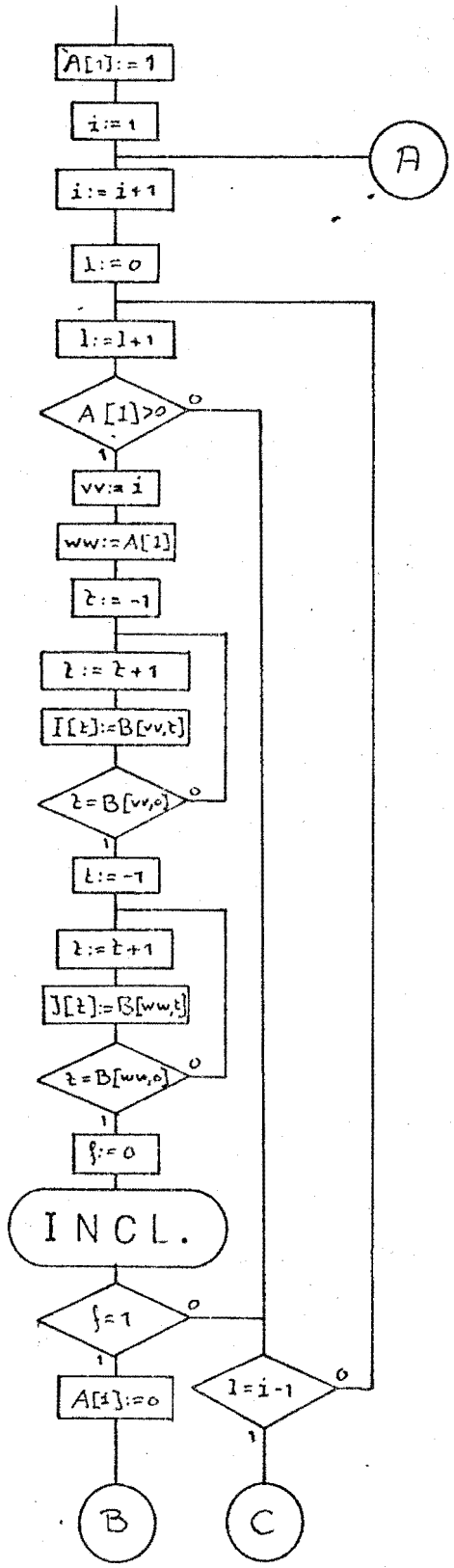
$ASS(C) := \{B_j \mid j \in J_n\}$ noemen we het met de overdekking C geassocieerde verzamelingensysteem van V.

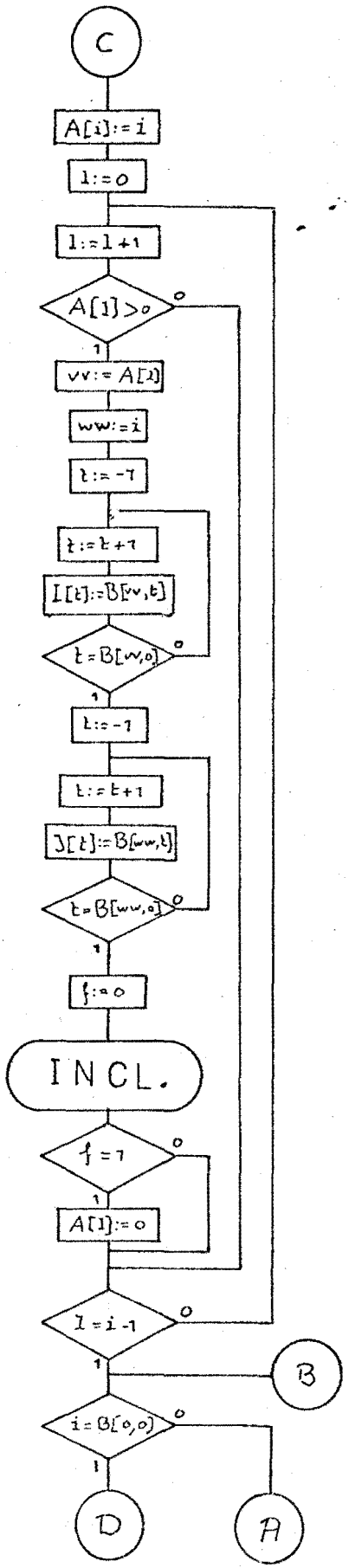
opm: ASS(C) is een verzamelingensysteem van V!

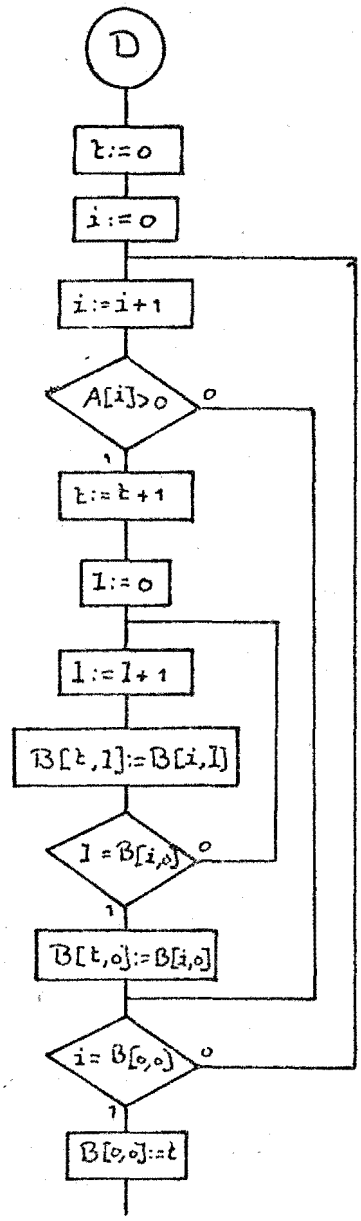
3.2. Het algoritme ASS

Bij 'begin' geldt: B[0,0]= aantal blokken van de overdekking C
B[i,0]= aantal elementen van het i-de blok van C
B[i,1]= het 1-ste element van het i-de blok van C
Bij 'einde' geldt: B[0,0]= |ASS(C)|
B[i,0]= aantal elementen van het i-de blok van ASS(C)
B[i,1]= het 1-ste element van het i-de blok van ASS(C)

opm: De elementen van de blokken zijn weer door positieve getallen gegeven.


A[1]:=1
i:=1
A
i:=i+1
l:=0
l:=l+1
A[l]>0
0
1
vv:=i
ww:=A[l]
t:=-1
t:=t+1
I[t]:=B[vv,t]
t=B[vv,0]
0
1
t:=-1
t:=t+1
J[t]:=B[ww,t]
t=B[ww,0]
0
1
f:=0
INCL.
f=1
0
1
A[i]:=0
l=i-1
0
1
B
C


C
A[i]:=i
l:=0
l:=l+1
A[l]>0
0
1
vv:=A[l]
ww:=i
t:=-1
t:=t+1
I[t]:=B[vv,t]
t=B[vv,0]
0
1
t:=-1
t:=t+1
J[t]:=B[ww,t]
t=B[ww,0]
0
1
f:=0
INCL.
f=1
0
1
A[l]:=0
l=i-1
0
1
B
i=B[0,0]
0
1
D
A


D
t:=0
i:=0
i:=i+1
A[i]>0
0
1
t:=t+1
l:=0
l:=l+1
B[t,l]:=B[i,l]
l=B[i,0]
0
1
B[t,0]:=B[i,0]
i=B[0,0]
0
1
B[0,0]:=t

3.3. Equivalentieklassen

3.3.1. μ is een verzamelingensysteem van V.
De relatie $R_\mu \subseteq V \times V$ wordt gedefinieerd door
$xR_\mu x' \Leftrightarrow \exists_{B \in \mu} [x \in B \wedge x' \in B]$ Notatie: $x \equiv x' \ (\mu)$

3.3.2. Als μ een partitie is, dan is R_μ een equivalentierelatie.

bewijs: $\bigcup_\mu B = V \Rightarrow \forall_{x \in V} \exists_{B \in \mu} [x \in B] \Rightarrow x \equiv x \ (\mu) \Rightarrow R_\mu$ is reflexief.
$xR_\mu y \Rightarrow \exists_{B \in \mu} [x \in B \wedge y \in B] \Rightarrow yR_\mu x \Rightarrow R_\mu$ is symmetrisch.

$xR_\mu y \wedge yR_\mu x \Rightarrow \exists_{B \in \mu} [x \in B \wedge y \in B] \wedge \exists_{B' \in \mu} [y \in B' \wedge z \in B'] \Rightarrow \exists_{B \in \mu} [x \in B \wedge z \in B] \Rightarrow xR_\mu z$
R_μ is transitief.

immers $\left.\begin{array}{l} y \in B \cap B' \\ B \neq B' \Rightarrow B \cap B' = \emptyset \end{array}\right\} \Rightarrow B = B'$

3.3.3. R is een equivalentierelatie over V.
$[x]_R := \{y \mid xRy\}$ oftewel $y \in [x]_R \Leftrightarrow xRy$
$[x]_R$ heet de equivalentieklasse van x.
De verzameling $\{[x]_R \mid x \in V\}$ is een partitie van V. Deze verzameling heet het quotiënt van V onder R en we geven haar aan met V/R.
$|V/R|$ heet de index van R over V.

bewijs: $\forall_{x \in V} [xRx] \Rightarrow \forall_{x \in V} [x \in [x]_R] \Rightarrow \bigcup_{x \in V} [x]_R = V$

Stel $\left.\begin{array}{l} [y]_R \cap [z]_R \neq \emptyset \Rightarrow \exists_{x \in V} [x \in [y]_R \wedge x \in [z]_R \\ [y]_R \neq [z]_R \Rightarrow \exists_{a \in V} [a \in [y]_R \wedge a \notin [z]_R] \end{array}\right\} \Rightarrow aRx \wedge \neg aRx$ (tegenspraak!)

dwz. $[y]_R \cap [z]_R \neq \emptyset \Rightarrow [y]_R \neq [z]_R$

3.3.4. R is een equivalentierelatie over V.
$[x]_R = [y]_R \Leftrightarrow xRy$

bewijs: $[x]_R = [y]_R \Rightarrow x \in [y]_R \Rightarrow xRy$

$xRy \Rightarrow \forall_{z \in [y]_R} [xRz] \Rightarrow \forall_{z \in [y]_R} [z \in [x]_R]$ idem: $\left.\begin{array}{l} [y]_R \subseteq [x]_R \\ [x]_R \subseteq [y]_R \end{array}\right\} [x]_R = [y]_R$

immers $z \in [y]_R$ betekent yRz; daar verder xRy verondersteld was, volgt uit de transitiviteit van R, dat xRz.

3.3.5. φ is een afbeelding van V in W.
De relatie $\varphi\varphi^{-1} = R$ is een equivalentierelatie over V.

bewijs: Volgens 2.3.5. geldt $D_V \subseteq R$ (reflexiviteit)
$R^{-1} = (\varphi\varphi^{-1})^{-1} = (\varphi^{-1})^{-1}\varphi^{-1} = \varphi\varphi^{-1} = R$ (symmetrie)
$R^2 = \varphi\varphi^{-1}\varphi\varphi^{-1} = \varphi D_W \varphi^{-1} = \varphi\varphi^{-1} = R$ (transitiviteit)

opm: Een equivalentieklasse van R bestaat uit die elementen van V die hetzelfde beeld in W hebben.

3.3.6. $(V, *)$ is een groepoïde.
$W_1 \subseteq V$ en $W_2 \subseteq V$.
$W_1 * W_2 := \{x * y \mid x \in W_1 \wedge y \in W_2\}$

3.3.6. $(V,*)$ is een groepoïde.
μ is een partitie van V.
μ heet toelaatbaar als
$\forall_{B_1\in\mu}\,\forall_{B_2\in\mu}\,\exists!_{B_3\in\mu}\,[B_1 * B_2 \subseteq B_3]$

3.3.7. $(V,*)$ is een groepoïde.
R is een congruentierelatie.
V/R is een toelaatbare partitie van V.

bewijs: We moeten bewijzen dat
$([x_1]_R=[y_1]_R) \wedge ([x_2]_R=[y_2]_R) \Rightarrow [x_1*y_1]_R=[x_2*y_2]_R$

$$\left.\begin{array}{l}[x_1]_R=[y_1]_R \Rightarrow x_1Ry_1\\ [x_2]_R=[y_2]_R \Rightarrow x_2Ry_2\end{array}\right\} \Rightarrow (x_1*y_1)R(x_2*y_2) \Rightarrow [x_1*y_1]_R=[x_2*y_2]_R$$

opm: Hiermee is tevens bewezen dat $(V/R,\overline{*})$ een groepoïde is, als $\overline{*}$ gedefinieerd wordt als $[x]_R\,\overline{*}\,[y]_R=[x*y]_R$

3.3.8. $(V,*)$ is een groepoïde.
μ is een toelaatbare partitie van V.
R_μ is een congruentierelatie.

bewijs: $$\left.\begin{array}{l}x_1R_\mu y_1 \Rightarrow \exists_{B\in\mu}\,[x_1\in B \wedge y_1\in B]\\ x_2R_\mu y_2 \Rightarrow \exists_{B'\in\mu}\,[x_2\in B' \wedge y_2\in B']\\ \mu \text{ is toelaatbaar}\end{array}\right\} \begin{array}{l}\Rightarrow (x_1*x_2)\in B*B'\\ \Rightarrow (y_1*y_2)\in B*B'\end{array} \left\}\begin{array}{l}\Rightarrow (x_1*x_2)\in B''\\ \Rightarrow (y_1*y_2)\in B''\end{array}\right\} \Rightarrow (x_1*x_2)R_\mu(y_1*y_2)$$
$$\exists!_{B''\in\mu}\,[B*B'\subseteq B'']$$

3.3.9. $(V,*)$ is een groepoïde.
R is een congruentierelatie.
Het groepoïde $(V/R,\overline{*})$ heet het factorgroepoïde van V over R.

3.3.10. $(V,*)$ is een groepoïde.
R is een congruentierelatie.
De afbeelding π van V op V/R met
$\forall_{x\in V}\,[\,x\pi=[x]_R\,]$
noemen we de natuurlijke afbeelding.
π is een homomorfisme.

bewijs:
Uit 3.3.7. $[x]_R\,\overline{*}\,[y]_R=[x*y]_R$
dus: $x\pi\,\overline{*}\,y\pi=(x*y)\pi$
Volgens 2.5.4. is π dan een homomorfisme.

3.3.11. $(V,*)$ is een groepoïde.
$(V',*')$ is een groepoïde.
φ is een homomorfisme van $(V,*)$ op $(V',*')$.

$\varphi\varphi^{-1}$ is een congruentierelatie R over V.
Er bestaat een isomorfisme Θ van V/R op V', zodat $\varphi=\pi\Theta$, waarbij π de natuurlijke afbeelding van V op V/R is.

bewijs: 3.3.5. $\Rightarrow$ R is een equivalentierelatie.
Omdat φ een homomorfisme is, geldt:
$aRb \Rightarrow a\varphi=b\varphi \Rightarrow (a\varphi)*'(c\varphi)=(b\varphi)*'(c\varphi) \Rightarrow (a*c)\varphi=(b*c)\varphi \Rightarrow a*cRb*c$
dus R is linkscongruent.
Op analoge wijze verkrijgt men de rechtscongruentie van R.
Volgens 2.5.7. is R een congruentierelatie.

Definieer nu $[a]_R\Theta = a\varphi$
(deze definitie is correct, immers $[a]_R = [b]_R \Rightarrow a\varphi = b\varphi$; zie opm in 3.3.5.)
Daar φ een surjectieve afbeelding is, is Θ een afbeelding van V/R op V'.
Θ is een homomorfisme:
$([a_1]_R \bar{*} [a_2]_R)\Theta = (a_1 * a_2)\varphi = a_1\varphi *' a_2\varphi = [a_1]_R\Theta *' [a_2]_R\Theta$
Θ is een-eenduidig:
$[a_1]_R\Theta = [a_2]_R\Theta \Leftrightarrow a_1\varphi = a_2\varphi \Leftrightarrow a_1 R a_2 \Leftrightarrow [a_1]_R = [a_2]_R$
Θ^{-1} is een homomorfisme:
$a_1\varphi\Theta^{-1} \bar{*} a_2\varphi\Theta^{-1} = [a_1]_R\Theta\Theta^{-1} \bar{*} [a_2]_R\Theta\Theta^{-1} = [a_1]_R \bar{*} [a_2]_R = [a_1 * a_2]_R = [a_1 * a_2]_R\Theta\Theta^{-1} = (a_1 * a_2)\varphi\Theta^{-1} = (a_1\varphi *' a_2\varphi)\Theta^{-1}$

Θ is dus een isomorfisme van $(V/R, \bar{*})$ op $(V', *')$
Ten slotte:
$a\varphi = [a]_R\Theta = (a\pi)\Theta = a\pi\Theta \Rightarrow \varphi = \pi\Theta$

3.3.12. $(V, *)$ is een groepoïde.
R_1 en R_2 zijn congruentierelaties en $R_1 \subseteq R_2$
$(V/R_2, \bar{*})$ is een homomorf beeld van $(V/R_1, \bar{*})$.

bewijs: $R_1 \subseteq R_2 \Rightarrow [a]_{R_1} \subseteq [a]_{R_2}$
We definiëren een afbeelding φ van V/R_1 op V/R_2:
$[a]_{R_1}\varphi = [a]_{R_2}$
Hiervoor geldt:
$[a_1]_{R_1}\varphi \bar{*} [a_1]_{R_1}\varphi = [a_1]_{R_2} \bar{*} [a_2]_{R_2} = [a_1 * a_2]_{R_2} = [a_1 * a_2]_{R_1}\varphi$
φ is dus een homomorfisme.

4. Semigroepen

4.1. Eenvoudige begrippen in de semigroepentheorie

4.1.1. $(S,*)$ is een groepoïde.
Als $*$ een associatieve produktoperatie is, dan noemen we $(S,*)$ een semigroep.
$|S|$ is de orde van de semigroep $(S,*)$.
$(S,*)$ noemen we eindig als $|S|$ eindig is.
Notatie: $a*a*\ldots*a = a^n$ $\quad a^n*a^m = a^{n+m}$
In deze paragraaf stelt $(S,*)$ steeds een semigroep voor.

4.1.2. Een element $i \in S$ heet idempotent als $i^2=i$

4.1.3. Een element $/e \in S$ heet een linkereenheid als $\forall_{s\in S}\ [/e*s=s]$
Een element $e/ \in S$ heet een rechtereenheid als $\forall_{s\in S}\ [s*e/=s]$

4.1.4. Een element $/o \in S$ heet een linkernulelement als $\forall_{s\in S}\ [/o*s=/o]$
Een element $o/ \in S$ heet een rechternulelement als $\forall_{s\in S}\ [s*o/=o/]$

4.1.5. /e, e/, /o en o/ zijn alle idempotent.

4.1.6. Als $(S,*)$ zowel een linker- als een rechtereenheid bevat, dan geldt:
$/e=e/:=e$.
We noemen e de eenheid van $(S,*)$.
$\forall_{s\in S}\ [e*s=s=s*e]$
Er is ten hoogste één eenheid in $(S,*)$.
Notatie: $s^\circ=e$.

bewijs: $e/=/e*e/=/e:=e$
Daar e een linkereenheid is, geldt $\forall_{s\in S}\ [e*s=s]$
Daar e een rechtereenheid is, geldt $\forall_{s\in S}\ [s*e=s]$
$\Big\}\ \forall_{s\in S}\ [e*s=s=s*e]$
Stel, ten slotte, dat zowel e_1 als e_2 eenheid in $(S,*)$ zijn, dan
$e_1=e_1*e_2=e_2$.

4.1.7. Als $(S,*)$ zowel een linker- als een rechternulelement bevat, dan geldt:
$/o=o/:=o$
o noemen we het nulelement van $(S,*)$.
$\forall_{s\in S}\ [o*s=o=s*o]$
Er is ten hoogste één nulelement in $(S,*)$.

bewijs: analoog aan het bewijs van 4.1.6.

4.1.8. $(S,*)$ heet een monoïde als
$\exists_{e\in S}\ \forall_{s\in S}\ [e*s=s=s*e]$

4.1.9. $(S,*)$ is een monoïde.
Een element $s_1 \in S$ heet een linkerinverse van $s \in S$ als $s_1*s=e$.
Een element $s_2 \in S$ heet een rechterinverse van $s \in S$ als $s*s_2=e$.
Een element $s^{-1} \in S$ heet de inverse van $s \in S$ als $s*s^{-1}=e=s^{-1}*s$.

4.1.10. $(S,*)$ is een monoïde.
Als een element $s \in S$ zowel een linker- als een rechterinverse heeft (resp. s_1 en s_2), dan heeft s een inverse s^{-1} en geldt: $s_1=s_2=s^{-1}$.
Een element heeft ten hoogste één inverse.
$(s^{-1})^{-1}=s$.
Notatie: $s^{-n}=(s^{-1})^n$

bewijs: $s_1=s_1*s*s_2=s_2$
Stel nu dat zowel r als t inversen van s in $(S,*)$ zijn, dan: $r=r*s*t=t$.

4.1.11. Een semigroep $(S,*)$ heet commutatief als de produktoperatie $*$ commutatief is.

4.1.12. $(T,*)$ heet een ondersemigroep van $(S,*)$ als
$T \subseteq S$
$T \neq \emptyset$
$\forall_{t_1 \in T} \; \forall_{t_2 \in T} \; [\, t_1 * t_2 \in T \,]$

$(T,*)$ heet een maximale, echte ondersemigroep als
$T \neq S \wedge T \subseteq V \subseteq S \wedge (V,*)$ is een ondersemigroep van $(S,*) \Rightarrow V=T \vee V=S$.

4.1.13. $X \subseteq S$
$(\langle X \rangle,*)$ is de 'kleinste' ondersemigroep van $(S,*)$ die X omvat.
$X \subseteq \langle X \rangle$
$(\langle X \rangle,*)$ noemen we de door X gegenereerde semigroep.
$(S,*)$ wordt door X gegenereerd als $\langle X \rangle = S$

$a \in S$: $(\langle a \rangle,*)$ is de cyclische ondersemigroep van $(S,*)$ die door a gegenereerd wordt. ($\langle a \rangle$ is een schrijfwijze voor $\langle \{a\} \rangle$)
$(S,*)$ heet cyclisch als $\exists_{a \in S} \; [\, S = \langle a \rangle \,]$

4.1.14. Het homomorfe beeld van een semigroep $(S,*)$ is weer een semigroep.

bewijs: We geven het homomorfisme dat S op S' afbeeldt aan met φ.
$(a\varphi *' b\varphi) *' c\varphi = (a*b)\varphi *' c\varphi = ((a*b)*c)\varphi = (a*(b*c))\varphi = a\varphi *' (b*c)\varphi = a\varphi *' (b\varphi *' c\varphi)$

4.1.15. Het beeld van een eventueel eenheidselement van $(S,*)$ onder een homomorfisme φ is een eenheid in $(S\varphi,*')$.
Hetzelfde geldt voor een linker- en rechtereenheid.

bewijs: $(e\varphi) *' (a\varphi) = (e*a)\varphi = a\varphi = (a*e)\varphi = a\varphi *' e\varphi$

4.1.16. Als a^{-1} de inverse van a is in $(S,*)$, dan is $(a^{-1})\varphi$ de inverse van $a\varphi$ in $(S',*')$, waarbij $S'=S\varphi$ en φ een homomorfisme is.

bewijs: $(a\varphi) *' (a^{-1}\varphi) = (a*a^{-1})\varphi = e\varphi = (a^{-1}*a)\varphi = (a^{-1}\varphi) *' (a\varphi)$
Volgens 4.1.15. is $e\varphi$ de eenheid van $(S',*')$.

4.1.17. $I \subseteq S$
$\forall_{i \in I} \; \forall_{s \in S} \; [\, i*s \in I \wedge s*i \in I \,]$ oftewel $I*S \subseteq I \wedge S*I \subseteq I$
I heet dan een ideaal van $(S,*)$.
I heet een linkerideaal als $S*I \subseteq I$.
I heet een rechterideaal als $I*S \subseteq I$.

opm: In alle drie de gevallen is $(I,*)$ een ondersemigroep van $(S,*)$.

4.1.18. Een semigroep $(T,*')$ 'deelt' de semigroep $(S,*)$, notatie $(T,*') \mid (S,*)$, als $(T,*')$ een homomorf beeld is van een ondersemigroep van $(S,*)$.

4.1.19. $(S,*) \mid (S,*)$

4.1.20. $(S,*)$, $(T,*')$ en $(U,*'')$ zijn semigroepen.
$(S,*)\mid(T,*') \wedge (T,*')\mid(U,*'') \Rightarrow (S,*)\mid(U,*'')$

bewijs: Er bestaat een ondersemigroep $(U',*''')$ van $(U,*'')$ en een afbeelding φ_1 van U' op T, zodat
$u'_1\varphi_1 *' u'_2\varphi_1 = (u'_1 *'' u'_2)\varphi_1$
Er bestaat een ondersemigroep $(T',*')$ van $(T,*')$ en een afbeelding φ_2 van T' op S, zodat
$t'_1\varphi_2 *' t'_2\varphi_2 = (t'_1 *' t'_2)\varphi$
$T'\varphi_1^{-1} = U''$, terwijl $(U'',*'')$ een ondersemigroep van $(U',*'')$ is.

$\exists_{u'_1 \in U'}[t'_1 = u'_1\varphi_1]$ en $\exists_{u'_2 \in U'}[t' = u'_2\varphi_1]$
Dit geeft ten slotte:
$u'_1\varphi_1\varphi_2 *'' u'_2\varphi_1\varphi_2 = t'_1\varphi_2 *' t'_2\varphi_2 = (t'_1 *' t'_2)\varphi_2 = (u'_1\varphi_1 *' u'_2\varphi_1)\varphi_2 = (u'_1 *'' u'_2)\varphi_1\varphi_2$
dwz. $\varphi_1\varphi_2$ is een homomorfisme van $(U'',*'')$ op $(S,*) \Rightarrow (S,*)\mid(U,*'')$.

4.1.21. $(S,*)$ en $(T,*')$ zijn semigroepen.
$(S,*)\mid(T,*') \wedge (T,*')\mid(S,*) \Rightarrow (S,*) \simeq (T,*')$

opm: We gebruiken het symbool $\simeq$ voor 'isomorf met'.

4.1.22. De verzameling van alle binaire relaties over een eindige verzameling V en produktvorming als operatie is een semigroep.

bewijs: 2.3.2.

4.2. Groepen

4.2.1. Een monoïde $(G,*)$ heet een groep als
$\forall_{a \in G} \exists_{b \in G} [b*a = e = a*b]$
het is duidelijk dat met b de inverse van a bedoeld wordt: $b = a^{-1}$

In deze paragraaf geeft $(G,*)$ steeds een groep aan.

4.2.2. In een groep $(G,*)$ hebben $a*x=b$ en $y*a=b$ elk één unieke oplossing in G.

bewijs: $x = a^{-1}*b$ is een oplossing van $a*x=b$, want $a*(a^{-1}*b) = (a*a^{-1})*b = e*b = b$.
Stel nu dat $c \in G$ een oplossing van $a*x=b$ is; dan $a*c=b \Rightarrow a^{-1}*(a*c) = a^{-1}*b \Rightarrow$
$\Rightarrow c = a^{-1}*b$.

$a^{-1}*b$ is dus de enige oplossing van $a*x=b$.

Zo is ook $b*a^{-1}$ de enige oplossing van $y*a=b$.

4.2.3. $(S,*)$ is een semigroep met $|S| \neq 0$.
$\forall_{a \in S} \forall_{b \in S} [|\{x \mid a*x=b\}| = 1 \wedge |\{y \mid y*a=b\}| = 1]$
Dan is $(S,*)$ een groep.

bewijs: Daar S niet leeg is, bestaat er een element a in S.
We geven de oplossing van $a*x=a$ met e_a aan.
Zowel e_a*b als b zijn oplossing van $a*x=a*b \Rightarrow \forall_{b \in S}[e_a*b=b]$
Zo geldt ook voor de oplossing van $y*a=a$: ae $\forall_{b \in S}[b*ae=b]$
Met 4.1.6. vinden we dan: $ae = e_a := e$

Neem nu een $c \in S$: $c*x=e$ heeft één oplossing d.
Nu geldt echter ook $d*c=e$, want $d*c$ en e zijn beide oplossing van $y*d=d$.

Hiermee is zowel de eenheid als de inverse aangetoond: $(S,*)$ is een groep.

4.2.4. Een groep heet commutatief als zijn produktoperatie commutatief is.

4.2.5. $H \subseteq G$ en $H \neq \emptyset$.
Als $(H,*)$ een groep is , dan noemen we $(H,*)$ een ondergroep van $(G,*)$.
Notatie: $(H,*) \lhd (G,*)$

4.2.6. $(H \subseteq G) \wedge (e \in H) \wedge (a \in H \Rightarrow a^{-1} \in H) \wedge (a \in H \wedge b \in H \Rightarrow a*b \in H) \Leftrightarrow (H,*) \lhd (G,*)$

bewijs:Uit de laatste van de vier beweringen links volgt dat $(H,*)$ een semigroep is als $H \neq \emptyset$.
Uit de tweede volgt dat $H \neq \emptyset$, en dat $(H,*)$ een monoïde is.
Uit de derde volgt dan ten slotte nog dat $(H,*)$ een groep is.

Het omgekeerde is triviaal.

4.2.7. $H \subseteq G$
$(H,*) \lhd (G,*) \Leftrightarrow (H \neq \emptyset) \wedge ((a \in H) \wedge (b \in H) \Rightarrow a*b^{-1} \in H)$

bewijs:Het bewijs van links naar rechts is triviaal.

Van rechts naar links gaat als volgt:
Omdat H niet leeg,is er een element a in H en dus: $a*a^{-1}=e \in H$
$b \in H \Rightarrow e*b^{-1} \in H \Rightarrow b^{-1} \in H$
$c \in H \wedge d \in H \Rightarrow c*(d^{-1})^{-1}=c*d \in H$

Volgens 4.2.6. is hiermee bewezen dat $(H,*) \lhd (G,*)$.

4.2.8. De doorsnede van een aantal ondergroepen van $(G,*)$ is een ondergroep van $(G,*)$

bewijs:$H = \cap H_\alpha$ met $(H_\alpha,*) \lhd (G,*)$.
Daar voor alle H_α : $e \in H_\alpha$ volgt daar uit dat $e \in \cap H_\alpha = H$.
$a \in H \Rightarrow \forall_{H_\alpha}[a \in H_\alpha]$ $\Big\}$ $\Rightarrow \forall_{H_\alpha}[a*b^{-1} \in H_\alpha] \Rightarrow a*b^{-1} \in H$
$b \in H \Rightarrow \forall_{H_\alpha}[b \in H_\alpha]$ $\Big\}$
Volgens 4.2.7. is $(H,*) \lhd (G,*)$.

4.2.9. $(G,*)$ heet cyclisch als
$\exists_{a \in G}[\langle a \rangle = G]$

4.2.10. $X \subset G$
Er bestaat een 'kleinste' ondergroep $(H,*)$ van $(G,*)$ waarvoor $X \subseteq H$.

bewijs:$\{H_\alpha \mid (H_\alpha,*) \lhd (G,*) \wedge X \subseteq H_\alpha\} \neq \emptyset$, want $(G,*) \lhd (G,*) \wedge X \subseteq G$.
We kiezen nu voor $(H,*)$ de groep $(\cap H_\alpha,*)$

Notatie: $(\langle X \rangle,*)$
$(\langle X \rangle,*)$ heet de door X gegenereerde ondergroep van G.

$X=\emptyset \Rightarrow \langle X \rangle = \{e\}$
$X \neq \emptyset \Rightarrow$ X = de verzameling van alle produkten van machten van elementen van X.

4.2.11. $(H,*) \lhd (G,*)$ en $t \in G$.
$H*t$ heet een rechternevenklasse van H; $t*H$ heet een linkernevenklasse van H.

opm: $H*t$ is een schrijfwijze voor $H*\{t\}$, evenals $t*H$ voor $\{t\}*H$.

4.2.12. $(H,*) \lhd (G,*)$
$H*t=H \Leftrightarrow t \in h \Leftrightarrow t*H=H$

bewijs: $t \in H \Rightarrow t^{-1} \in H \Rightarrow \forall_{h \in H} [h*t^{-1} \in H] \Rightarrow \forall_{h \in H} [h*t^{-1}*t=h \in H*t]$

$\left.\begin{array}{l} t \notin H \\ e \in H \Rightarrow t=e*t \in H*t \end{array}\right\} \Rightarrow H*t \neq H$

Analoog voor linkernevenklassen.

4.2.13. $(H,*) \lhd (G,*)$
$H*H=H$

bewijs: 4.2.12. $\Rightarrow \left.\begin{array}{l} \forall_{t \in H} [H*t=H] \\ H*H=\bigcup_{t \in H} H*t \end{array}\right\} \Rightarrow H*H=\bigcup_{t \in H} H=H.$ (4.2.12)

4.2.14. $H \subseteq G \wedge |H|$ is eindig $\wedge H*H=H \Rightarrow (H,*) \lhd (G,*)$

bewijs: $a \in H \Rightarrow <a> \subseteq H.$
Daar H eindig is, zijn er machten van a gelijk:
$(s < t)\ a^s=a^t \Rightarrow \left.\begin{array}{l} a^{t-s}=e \in H \\ a^{t-s-1}=a^{-1} \in H \end{array}\right\} \Rightarrow (H,*) \lhd (G,*).$
$a \in H \wedge b \in H \Rightarrow a*b \in H*H=H$

4.2.15. $(H,*) \lhd (G,*)$
$\forall_{t \in G} [|H|=|H*t|]$

bewijs: $h_1*t=h_2*t \Rightarrow h_1=h_2$ (4.2.2.)

4.2.16. $(H,*) \lhd (G,*)$, $a \in G$ en $b \in G$.
$H*a=H*b \Leftrightarrow a*b^{-1} \in H$
$a*H=b*H \Leftrightarrow a^{-1}*b \in H$

bewijs: $H*a=H*b \Rightarrow a \in H*b \Rightarrow \exists_{h \in H} [h*b=a] \Rightarrow h=a*b^{-1} \in H$

$\exists_{h \in H} [a*b^{-1}=h] \Rightarrow a=h*b \Rightarrow H*a=H*h*b=H*b.$ (4.2.12.)

4.2.17. De rechternevenklassen van een ondergroep $(H,*)$ van $(G,*)$ vormen een partitie van G.
Hetzelfde geldt voor de linkernevenklassen.

bewijs: $x \in H*a \cap H*b \Rightarrow \exists_{h_1 \in H} \exists_{h_2 \in H} [x=h_1*a=h_2*b] \Rightarrow a*b^{-1}=h_1^{-1}*h_2 \in H \Rightarrow H*a=H*b$ (4.2.16.)

Elk element c van G is in tenminste één blok bevat, want $c \in H*c$ $(e \in H!)$.

4.2.18. $(H,*) \lhd (G,*)$
Het aantal rechternevenklasse van $(H,*)$ in $(G,*)$ is gelijk aan het aantal linkernevenklassen van $(H,*)$ in $(G,*)$.

bewijs: Als $|G|$ eindig is, volgt de stelling uit 4.2.15. en 4.2.17.
Voor het voor ons onbelangrijke geval dat $|G|$ niet eindig is, merken we op, dat de relatie R
$(H*a)R(a^{-1}*H)$
een-eenduidig is; immers uit 4.2.16. volgt: $H*a=H*b \Leftrightarrow a^{-1}*H=b^{-1}*H.$

4.2.19. $(H,*) \lhd (G,*)$
Het aantal rechternevenklassen van $(H,*)$ in $(G,*)$ noemen we de index van $(H,*)$ in $(G,*)$.
Notatie: $[G:H]$

4.2.20. $(H,*) \lhd (G,*)$
Als $|G|$ eindig is, dan $[G:H]=|G|/|H|$.

bewijs: 4.2.15. en 4.2.17.

4.2.21. $a \in G$
$|<a>|$ noemen we de orde van a.

4.2.22. $a \in G$
De orde van a deelt $|G|$, als $|G|$ eindig is

bewijs: $(<a>,*)$ is een ondergroep van $(G,*)$.
Uit 4.2.15. en 4.2.17. volgt dan de stelling.

4.2.23. De relatie γ_a die gedefinieerd wordt door
$\forall_{x \in G} [(x, a*x*a^{-1}) \in \gamma_a]$ waarbij $a \in G$ is, heet conjugatie.
$a*x*a^{-1}$ heet de geconjugeerde van x door a.

4.2.24. γ_a is een automorfisme.

bewijs: γ_a is een homomorfisme:
$x\gamma_a * y\gamma_a = (a*x*a^{-1})*(a*y*a^{-1}) = (a*x)*(a^{-1}*a)*(y*a^{-1}) = a*(x*y)*a^{-1} = (x*y)\gamma_a$

γ_a is een een-eenduidige afbeelding van G op G. (4.2.2.)
γ_a^{-1} is ook een homomorfisme, immers $\forall_{x \in G} [(x, a^{-1}*x*a) \in \gamma_a^{-1}]$
γ_a is dus een isomorfisme van $(G,*)$ op zichzelf, en dus een automorfisme.

4.2.25. $(H,*) \lhd (G,*)$
$(H,*)$ heet normaal als
$\forall_{g \in G} [g*H*g^{-1}=H]$
Notatie: $(H,*) \lhd\!\lhd (G,*)$

4.2.26. $(H,*) \lhd (G,*)$
Als $(G,*)$ commutatief is, dan $(H,*) \lhd\!\lhd (G,*)$

bewijs: $g*h*g^{-1}=g*g^{-1}*h=h$. Omkering van de stelling is onjuist!

4.2.27. $(H,*) \lhd\!\lhd (G,*) \Leftrightarrow \forall_{g \in G} [g*H=H*g]$

bewijs: $g*H*g^{-1}=H \Leftrightarrow g*H=H*g$

4.2.28. $(H,*) \lhd\!\lhd (G,*)$, $g \in G$ en $h \in H$.
$\exists_{h' \in H} [g*h=h'*g]$

bewijs: 4.2.27.

4.2.29. De doorsnede van een aantal normale ondergroepen van $(G,*)$ is een normale ondergroep van $(G,*)$.

bewijs: $H = \bigcap H_\alpha$ en $\forall_{H_\alpha} \forall_{g \in G} [g*H_\alpha*g^{-1}=H_\alpha]$
Uit 4.2.8. weten we dat $(H,*)$ een ondergroep van $(G,*)$ is.

$h \in H \Leftrightarrow \forall_{H_\alpha} [h \in H_\alpha] \Leftrightarrow \forall_{H_\alpha} [g*h*g^{-1} \in H_\alpha] \Leftrightarrow g*h*g^{-1} \in H$

(Equivalenties omdat γ_g een-eenduidig is)

4.2.30.Het homomorfe beeld van een groep is weer een groep.

bewijs:4.1.14., 4.1.15. en 4.1.16.

4.2.31.Als R een congruentierelatie is, dan $([e]_R,*) \lhd (G,*)$.

bewijs: $\left.\begin{array}{l} a \in [e]_R \\ b \in [e]_R \end{array}\right\} \Rightarrow [a*b^{-1}]_R = [a*b^{-1}*e]_R = [a*b^{-1}*b]_R = [a]_R = [e]_R$

dwz. $a*b^{-1} \in [e]_R \Rightarrow ([e]_R,*) \lhd (G,*)$

$b \in [a]_R \Rightarrow [a*b^{-1}]_R = [a^{-1}*a]_R = [e]_R \Rightarrow a^{-1}*b \in [e]_R \Rightarrow a*a^{-1}*b = b \in a*[e]_R$
$b \in a*[e]_R \Rightarrow [a*b^{-1}]_R = [e]_R \Rightarrow (a*b)Re \Rightarrow bRa \Rightarrow b \in [a]_R$
$\Rightarrow [a]_R = a*[e]_R$
idem $[a]_R = [e]_R*a$

dwz. $([e]_R,*) \lhd (G,*)$

4.2.32.Als R een congruentierelatie is, dan $[g]_R = g*[e]_R = [e]_R*g$.

bewijs:4.2.31. en 4.2.27.

4.2.33.$(G/R,\overline{*})$ is een groep.

bewijs:De natuurlijke afbeelding van G op G/R is een homomorfisme (3.3.10).
Uit 4.2.30. volgt dan dat $(G/R,\overline{*})$ een groep is.

$(G/R,\overline{*})$ wordt ook wel genoteerd als $(G/H,\overline{*})$, waarbij $H=[e]_R$.
We noemen haar de factorgroep.
Haar orde is $|G|/|H| = [G:H]$.
Haar elementen zijn de nevenklassen.

4.2.34. φ is een homomorfisme van $(G,*)$ op $(G',*')$.
$[e]_{\varphi\varphi^{-1}}$ heet dan de kern van het homomorfisme φ en $(G/[e]_{\varphi\varphi^{-1}},\overline{*}) \simeq (G',*')$.

bewijs:3.3.11.

4.2.35.$(H,*) \lhd (G,*)$
Er bestaat een groep en een homomorfisme van $(G,*)$ op die groep, waarvan de kern precies H is.

bewijs:
Definieer φ als de afbeelding die aan elke $g \in G$ de nevenklasse $H*g$ toevoegt.
De rest volgt uit 4.2.31. t/m 4.2.34.

4.2.36.$(H,*) \lhd (G,*) \wedge (K,*) \lhd (G,*) \Rightarrow (K*H,*) \lhd (G,*)$.

bewijs: $\left.\begin{array}{l} a \in K*H \Rightarrow \exists_{k_1 \in K} \exists_{h_1 \in H} [a=k_1*h_1] \\ b \in K*H \Rightarrow \exists_{k_2 \in K} \exists_{h_2 \in H} [b=k_2*h_2] \end{array}\right\} \Rightarrow a*b^{-1} = k_1*(h_1*h_2^{-1})*k_2^{-1}$

Daar $(K,*) \lhd (G,*)$ geldt: $g=h_1*h_2^{-1}*k_2^{-1}*(h_1*h_2^{-1})^{-1} \in K$ (immers volgens 4.2.25. geldt: $g*K*g^{-1}=K$). Invullen geeft:
$a*b^{-1} = (k_1*g)*(h_1*h_2^{-1}) \in K*H \Rightarrow (K*H,*) \lhd (G,*)$.

4.2.37.$(H,*) \lhd (G,*) \wedge (K,*) \lhd (G,*) \Rightarrow (K*H,*) \lhd (G,*)$.

We weten uit 4.2.36. dat $(K*H,*) \lhd (G,*)$.
Omdat $(K,*)$ en $(H,*)$ beide normale ondergroepen van $(G,*)$ zijn, geldt voor alle $g \in G$:
$g*K*H*g^{-1} = g*K*e*H*g^{-1} = g*K*g^{-1}*g*H*g^{-1} = K*H$. Dus $(K*H,*) \lhd (G,*)$.

4.2.38. $(H,*)\lhd(G,*) \wedge (K,*)\blacktriangleleft(G,*) \Rightarrow (H\cap K,*)\blacktriangleleft(H,*) \wedge (H/H\cap K,\overline{*}) \simeq (H*K/K,\overline{*})$

bewijs: π is de natuurlijke afbeelding van G op G/K.
Dan is $D_H\pi$ een homomorfisme van $(H,*)$ in $(G/K,\overline{*})$ met als kern $H\cap K$.
Uit 4.2.31 volgt dan $(H\cap K,*)\blacktriangleleft(H,*)$ en uit 4.2.34. $(H/H\cap K,\overline{*})\simeq(H(D_H\pi),\overline{*})$,
terwijl $H(D_H\pi)$ juist $H*K/K$ is.

4.2.39. $K\subseteq H\subseteq G$.
$(K,*)\lhd(G,*)$, $(H,*)\blacktriangleleft(G,*)$ en $(K,*)\blacktriangleleft(H,*)$.
$(H/K,\overline{*})\blacktriangleleft(G/K,\overline{*})$ en $((G/K)/(H/K),\overline{\overline{*}})\simeq(G/H,\overline{*})$

bewijs: φ is de afbeelding van G/K op G/H met $(K*a)\varphi = H*a$
De kern van φ is H/K.
De rest van de stelling volgt nu uit 4.2.31. t/m 4.2.34.

4.2.40. $(K,*)\lhd(G,*)$, $(K',*)\lhd(G,*)$ en $(K',*)\blacktriangleleft(K,*)$.
$(H,*)\lhd(G,*)$, $(H',*)\lhd(G,*)$ en $(H',*)\blacktriangleleft(H,*)$.

Nu geldt: $(K'*(K\cap H'),*)\blacktriangleleft(K'*(K\cap H),*)$
$(H'*(K'\cap H),*)\blacktriangleleft(H'*(K\cap H),*)$
$(K'*(K\cap H)/K'*(K\cap H'),\overline{*})\simeq(H'*(K\cap H)/H'*(K'\cap H),\overline{*})$

bewijs: $D=(K\cap H')*(H\cap K')$
4.2.8. $\Rightarrow (K\cap H,*)\lhd(G,*)\Rightarrow(K\cap H,*)$ is een groep.
$g\in D \Rightarrow g=g_1*g_2$ met $\left.\begin{matrix} g_1\in K \wedge g_1\in H \\ g_2\in H \wedge g_2\in K\end{matrix}\right\} \Rightarrow g\in K\cap H \Rightarrow D\subseteq K\cap H$

$$\left.\begin{matrix}(K\cap H,*)\lhd(H,*)\\ (K\cap H)\cap H'=K\cap H'\\ (H',*)\blacktriangleleft(H,*)\end{matrix}\right\}\Rightarrow\left.\begin{matrix}(K\cap H',*)\blacktriangleleft(K\cap H,*)\\ (4.2.38.)\\ (K'\cap H,*)\blacktriangleleft(K\cap H,*)\end{matrix}\right\}\Rightarrow(D,*)\blacktriangleleft(K\ \ H,*)\qquad(4.2.36.)$$

Volgens 4.2.33. is dan $(K\cap H/D,\overline{*})$ een groep.

$$\left.\begin{matrix}(K',*)\blacktriangleleft(K,*)\\ (K\cap H,*)\lhd(K,*)\end{matrix}\right\}\Rightarrow(K'*(K\cap H),*)\lhd(K,*)\qquad(4.2.36.)$$

Elk element van $K'*(K\cap H)$ is te schrijven als $k'*c$ met $k'\in K'$ en $c\in(K\cap H)$

We definiëren een relatie $\Psi\subseteq(K'*(K\cap H))\times(K\cap H/D)$: $(k'*c)\Psi(D*c)$
Stel nu: $k'*c=k_1'*c_1$ met ook $k_1'\in K'$ en $c_1\in K\cap H$.
dan: $(k_1')^{-1}*k'=c_1*c^{-1}\in K'\cap(K\cap H)=K'\cap H\subseteq D$
Hieruit volgt dat Ψ een surjectieve afbeelding van $K'*(K\cap H)$ op $K\cap H/D$ is.
Ψ is ook een homomorfisme, want $k_1'*c_1*k_2'*c_2=k_3'*c_1*c_2$ met $k_3'=k_1'*c_1*k_2'*c_1^{-1}$.
$(k_3'\in K'$, omdat $(K',*)\blacktriangleleft(K\cap H,*))$.
Daar $K\cap H'\subseteq(K\cap H')*(H\cap K')=D$ moet $K'*(K\cap H')\subseteq$ kern(Ψ). (4.2.12.)
Stel nu: $(k'*c)\Psi=D\Rightarrow c\in D\Rightarrow c=u*v$ met $u\in H\cap K'$ en $v\in K\cap H'$.
Dus: $k'*c=k'*u*v=k_1'*v\in K'*(K\cap H')\Rightarrow$ kern$(\Psi)\subseteq K'*(K\cap H')$.
Hiermee is bewezen dat kern$(\Psi)=K'*(K\cap H')$.

Volgens 4.2.31. en 4.2.34. geeft dit: $(K'*(K\cap H'),*)\blacktriangleleft(K'*(K\cap H),*)$
$(K'*(K\cap H)/K'*(K\cap H'),\overline{*})\simeq(K\cap H/D,\overline{*})$.
Op analoge wijze vindt men: $(H'*(K'\cap H),*)\blacktriangleleft(H'*(K\cap H),*)$
$(H'*(K\cap H)/H'*(K'\cap H),\overline{*})\simeq(K\cap H/D,\overline{*})$.
Daar isomorfie een equivalentierelatie is, is het bewijs nu compleet.

4.2.41.$(G,*)$ heet enkelvoudig als ze geen andere normale ondergroepen heeft als $(\{e\},*)$ en $(G,*)$.

4.2.42.Als $|G|$ een priemgetal is, dan is $(G,*)$ enkelvoudig.

bewijs:Als $(H,*) \triangleleft (G,*)$, dan $|H| \mid |G|$.
$|G|$ is echter een priemgetal en heeft dus geen echte delers.

4.2.43.Een normaalrij van een groep $(G,*)$ is een rij groepen, $(G_0,*), (G_1,*), \ldots$ $\ldots (G_k,*)$, waarvoor geldt:
$(G,*) \simeq (G_0,*) \triangleright (G_1,*) \triangleright \ldots\ldots \triangleright (G_k,*) \simeq (\{e\},*)$.
De groepen $(G_i/G_{i+1},\overline{*})$ heten de factoren van de normaalrij.

4.2.44.De normaalrij $(G'_0,*), (G'_1,*), \ldots\ldots (G'_n,*)$ van $(G,*)$ heet een verfijning van de normaalrij $(G_0,*), (G_1,*), \ldots\ldots (G_k,*)$ van $(G,*)$ als
$\forall_{(G_i,*)} \; \exists_{(G'_j,*)} \left[(G_i,*)=(G'_j,*)\right]$
De verfijning heet echt als
$\exists_{(G'_j,*)} \; \forall_{(G_i,*)} \left[(G_i,*)\neq(G'_j,*)\right]$

4.2.45.Twee normaalrijen heten equivalent als hun factoren in een een-eenduidige correspondentie gebracht kunnen worden, zodat de corresponderende factoren isomorf zijn.

4.2.46.Een normaalrij van $(G,*)$ die geen isomorfe groepen bevat en geen echte verfijningen heeft, heet een compositierij van $(G,*)$.

4.2.47.Elke eindige groep heeft een compositierij.

4.2.48.Bij elk paar normaalrijen van $(G,*)$ bestaat een paar equivalente verfijningen.

bewijs:$(G_0,*), (G_1,*), \ldots\ldots (G_k,*)$ en $(G'_0,*), (G'_1,*), \ldots\ldots (G'_n,*)$ zijn normaalrijen van $(G,*)$.
Tussen $(G_i,*)$ en $(G_{i+1},*)$ voegen we de groepen $(G_{i+1}*(G_i \cap G'_j),*)$ met $0 \leq j \leq n$ in.
Tussen $(G'_i,*)$ en $(G'_{i+1},*)$ voegen we de groepen $(G'_{i+1}*(G'_i \cap G_j),*)$ met $0 \leq j \leq k$ in.

Volgens de eerste twee beweringen van 4.2.40. zijn de aldus gevormde rijen verfijningen van de oorspronkelijke.
Volgens de derde bewering van 4.2.40. zijn ze ook equivalent.

4.2.49.Elk paar compositierijen van $(G,*)$ is equivalent.

bewijs:Volgt direkt uit 4.2.48.

4.2.50.Een normaalrij van $(G,*)$ is een compositierij slals elke factor enkelvoudig is.

bewijs:Stel $(G_{i+1},*) \triangleleft (G_i,*)$ kan verfijnd worden door tussenvoegen van $(H,*)$:
$(G_{i+1},*) \triangleleft\!\!\!\neq (H,*) \triangleleft\!\!\!\neq (G_i,*)$. Volgens 4.2.39. geldt dan echter:
$(\{e\},\overline{*}) \triangleleft\!\!\!\neq (H/G_{i+1},\overline{*}) \triangleleft\!\!\!\neq (G_i/G_{i+1},\overline{*})$. Maar dan kan $(G_i/G_{i+1},\overline{*})$ niet enkelvoudig zijn.
Omgekeerd: Als $(G_i/G_{i+1},\overline{*})$ niet enkelvoudig is, dan is er een $(K,*)$, zodat $(\{e\},\overline{*}) \triangleleft\!\!\!\neq (K,\overline{*}) \triangleleft\!\!\!\neq (G_i/G_{i+1},\overline{*})$.
Laat π_i nu de natuurlijke afbeelding van G_i op G_i/G_{i+1} zijn.
Dan volgt direkt: $(G_{i+1},*) \triangleleft (K\pi_i^{-1},*) \triangleleft (G_i,*)$ is een echte verfijning.

4.2.51. $(K,*')$ is een enkelvoudige groep.
φ is een homomorfisme van G op K.
$(H,*) \lhd (G,*)$.
Dan geldt: $H\varphi = e_K \vee H\varphi = K$

bewijs: $H\varphi = K'$.
Daar $(K',*')$ een homomorf beeld van de groep $(H,*)$ is, is $(K',*')$ een ondergroep van $(K,*')$.
We kunnen voor elke $k \in K$ een $g \in k\varphi^{-1}$ nemen.
$(H,*)$ is een normale ondergroep van $(G,*) \Rightarrow g*H*g^{-1}=H \Rightarrow g\varphi *' H\varphi *' g^{-1}\varphi \Rightarrow$
$\Rightarrow k*'K'*'k^{-1}=K'$.
Daar dit voor elke $k \in K$ geldt, is $(K',*')$ een normale ondergroep van $(K,*')$.
$(K,*')$ is echter enkelvoudig, dus $K'=H\varphi = e_K$ of K.

4.2.52. $(K,*')$ is een enkelvoudige groep.
φ is een homomorfisme van G op K.
$(H,*) \lhd (G,*)$.
Dan geldt: $(K,*')$ is een homomorf beeld van $(H,*)$ of van $(G/H,\overline{*})$

bewijs: Als $H\varphi = K$, dan is de bewering triviaal. Volgens 4.2.51 blijft dan nog slechts $H\varphi = e_K$ over; dwz: $H \subseteq \text{kern}(\varphi)$.
Daar $(H,*) \lhd (G,*)$, geldt $(H,*) \lhd (\text{kern}(\varphi),*)$.
Dit betekent dat de congruentierelaties, geïnduceerd door de partities bestaande uit de nevenklassen van H in G resp. de nevenklassen van $\text{kern}(\varphi)$ in G, voldoen aan de voorwaarde van stelling 3.3.12.
Dus $(G/\text{kern}(\varphi),\overline{*})$ is een homomorf beeld van $(G/H,\overline{*})$.
Daar bovendien $(K,*') \simeq (G/\text{kern}(\varphi),\overline{*})$ (4.2.34.), volgt dat $(K,*')$ een homomorf beeld van $(G/H,\overline{*})$ is.

4.2.53. $(G_1,*)$ en $(G_2,*')$ zijn groepen.
Het direkt produkt $(G_1 \times G_2, \underline{*})$ van $(G_1,*)$ en $(G_2,*')$ is gedefinieerd door:
$(g_1,g_2) \in G_1 \times G_2 \wedge (g_1',g_2') \in G_1 \times G_2 \Rightarrow (g_1,g_2)\underline{*}(g_1',g_2') = (g_1 * g_1', g_2 *' g_2')$

4.2.54. $(G_1 \times G_2, \underline{*})$ is een groep.

bewijs: Het is duidelijk dat $(G_1 \times G_2, \underline{*})$ een semigroep is. Bovendien is (e_1,e_2) eenheid in deze semigroep en is (g_1^{-1},g_2^{-1}) de inverse van (g_1,g_2).

4.2.55. $(G_1,*)$ en $(G_2,*')$ zijn groepen.
$(G_1 \times \{e_2\}, \underline{*}) \lhd (G_1 \times G_2, \underline{*})$ en $(G_1 \times \{e_2\}, \underline{*}) \simeq (G_1,*)$.
$(\{e_1\} \times G_2, \underline{*}) \lhd (G_1 \times G_2, \underline{*})$ en $(\{e_1\} \times G_2, \underline{*}) \simeq (G_2,*')$.

4.2.56. $(G_1,*')$ en $(G_2,*'')$ zijn groepen.
$(G,*)$ noemen we een uitbreiding van $(G_1,*')$ met $(G_2,*'')$ als
$(G_1,*') \lhd (G,*) \wedge (G/G_1,\overline{*}) \simeq (G_2,*'')$.

4.2.57. $(G_1,*)$ en $(G_2,*')$ zijn groepen.
$(K,\underline{*}) \lhd (G_1 \times G_2, \underline{*})$
Dan is $(K,\underline{*})$ een uitbreiding van een groep isomorf aan een ondergroep $(G_1',*)$ van $(G_1,*)$ met een groep isomorf aan een ondergroep $(G_2',*')$ van $(G_2,*')$.

bewijs: $K' = \{(g_1,e_2) \mid (g_1,e_2) \in K\}$
$(K',\underline{*}) \lhd (K,\underline{*})$ en $(K',\underline{*}) \simeq (G_1',*)$ (waarmee we $(G_1',*)$ vastleggen)

Welnu: $(g_1,g_2) \in K'\underline{*}(g_1',g_2') \Leftrightarrow g_2 *' (g_2')^{-1} = e_2 \Rightarrow g_2 = g_2'$.
Dus elke rechternevenklasse van K' in K wordt door de tweede component bepaald $\Rightarrow (K/K',\overline{\underline{*}}) \simeq (G_2',*')$.

4.2.58. $(G_1,*)$ en $(G_2,*')$ zijn groepen.
$(K,\underline{*}) \lhd (G_1 \times G_2, \underline{*})$
φ is een homomorfisme van K op een enkelvoudige groep $(H,\times)$.
Dan is $(H,\times)$ een homomorf beeld van $(G_1',*)$ of van $(G_2',*')$, waarbij $(G_1',*)$ een ondergroep van $(G_1,*)$ is en $(G_2',*')$ van $(G_2,*')$.

bewijs: 4.2.52. en 4.2.57.

4.2.59. Alle permutaties over een eindige, niet-lege verzameling V vormen een groep, die we de symmetrische groep noemen.

bewijs: Natuurlijk is het produkt van twee permutaties weer een permutatie.
Volgens 2.3.2. is produktvorming associatief.
De identiteit is een permutatie.
Volgens 2.2.7. is de inverse van een permutatie weer een permutatie.

4.2.60. X is een niet-lege verzameling van permutaties over V met $|V|$ eindig.
$(\langle X\rangle,)$ is een groep.

bewijs: $(\langle X\rangle,)$ is een semigroep (2.3.2.)
$\varphi \in \langle X\rangle \Rightarrow \bigwedge_{p\in\mathbb{N}} [\varphi^p \in \langle X\rangle]$
Er zijn slechts eindig veel permutaties over V mogelijk $\Rightarrow \varphi^s = \varphi^t$ voor een s en t met $s \neq t$
Stel $s < t \Rightarrow \varphi^{t-s}$=identiteit en φ^{t-s-1} is de inverse van φ.

4.2.61. V is een eindige verzameling.
(G,) is een groep van permutaties over V.
Dan is $\mu = \{vG \mid v \in V\}$ een partitie van V.
De elementen van μ heten de banen van V.
Als $|\mu|=1$, dan heet de groep (G,) transitief.

bewijs: $vR_\mu v' \Leftrightarrow \bigvee_{\varphi\in G} [v\varphi = v']$

$vR_\mu v' \Rightarrow \bigvee_{\varphi\in G} [v\varphi = v'] \Rightarrow v'\varphi^{-1} = v \Rightarrow v'R_\mu v$ (reflexiviteit)
$D_v \in G \Rightarrow vR_\mu v$ (symmetrie)
$vR_\mu v' \wedge v'R_\mu v'' \Rightarrow \bigvee_{\varphi\in G} [v\varphi = v'] \wedge \bigvee_{\varphi'\in G} [v'\varphi' = v''] \Rightarrow v\varphi\varphi' = v'' \Rightarrow vR_\mu v''$
(transitiviteit).

4.3. Stellingen over eindige semigroepen

4.3.1. Een semigroep (S,*) is een groep slals ze geen echte linker- of rechteridealen heeft.

bewijs: Als (S,*) geen echte linker- of rechteridealen heeft, dan
$\bigwedge_{a\in S} [a*S=S=S*a]$ (anders zou S*a een linker- en a*S een rechterideaal zijn).
Dus $\bigvee_{b\in S} [b*a=a]$
Neem nu een $c \in S$, waarvoor a*z=c, dan b*c=b*a*z=a*z=c.
b is dus een rechtereenheid. Op deze manier vinden we ook een linkereenheid en we kunnen concluderen dat (S,*) een monoïde is.
Voor alle a S moet ook gelden: $\bigvee_{a'\in S} [a*a'=e]$; dwz. a heeft een rechterinverse. Zo ook een linkerinverse. Ergo, elk element van S heeft een inverse.

De omkering volgt direkt uit oa. 4.2.12.: $\bigwedge_{g\in G} [g*G=G=G*g]$

4.3.2. $(S,*)$ is een eindige semigroep en $a \in S$.
Er bestaan twee positieve getallen bij a, de zgn. index r en periode m, zodat: $a^r = a^{r+m}$.
$\langle a \rangle = a, a^2, \ldots, a^{m+r-1}$
$(\{a, a^2, \ldots, a^{r+m-1}\}, *)$ is een cyclische ondergroep van $(S,*)$
$n \equiv 0 \pmod m \wedge (r \leq n \leq m+r-1) \Rightarrow a^n$ is idempotent en a^n is de eenheid van de genoemde groep.

bewijs: Daar S eindig is, bestaat er een r en een t, zodat $a^r = a^t$, $t > r$, terwijl t de eerste exponent is waarvoor zo'n geval zich voordoet.
Noem $t-r$ voortaan m.
Dan $a^r = a^{r+m} = a^r * a^m = a^{r+m} * a^m = \ldots = a^{r+q.m}$ voor alle $q > 0$.

Volgens de reststelling is elk positief geheel getal $k \geq r+m$ eenduidig te schrijven als $r+q.m+p$ met $0 \leq p < m$.
$a^k = a^{r+q.m+p} = a^{r+p}$
Dwz. dat elke a^k met $k \geq r$ gelijk is aan een a^{r+p} met $0 \leq p < m$. Dit betekent dat $\{a, a^2, \ldots, a^{r-1}, a^r, a^{r+1}, \ldots, a^{r+m-1}\}$ alle elementen van $\langle a \rangle$ bevat.

De verzameling $a^r, a^{r+1}, \ldots, a^{r+m-1}$ noemen voortaan K.
Zoals reeds bleek is K gesloten voor de operatie $* \Rightarrow (K,*)$ is een semigroep.
De getallen n met $r \leq n \leq m+r-1$ vormen een volledig restsysteem mod m. Er is dus ook een $n \equiv 0 \pmod m$. Voor deze n geldt:
$a^{r+p} * a^n = a^{r+p} * a^{x.m} = a^{r+x.m+p} = a^{r+p}$. a^n is een eenheid in $(K,*)$.
Verder kan men voor elke p een y kiezen, zodat $y.m-r-p > r$ en $y > n/m = x$:
$a^{r+p} * a^{y.m-r-p} = a^{r+(y-x)m+x.m+p-r-p} = a^{r+x.m+p-r-p} = a^n$.
Dus a^{r+p} en $a^{y.m-r-p}$ zijn elkaars inverse.

Hiermee is bewezen dat $(K,*)$ een groep is. $(K,*)$ is ook cyclisch, want $K = \langle a^{n+1} \rangle$.

opm. Elke cyclische semigroep is commutatief!

4.3.3. Elke eindige semigroep bevat ten minste één idempotent element.

bewijs: 4.3.2.

4.3.4. $(S,*)$ is een eindige semigroep en $(G,*)$ is een eindige groep.
Als $(G,*) \mid (S,*)$, dan bestaat er een ondergroep $(K,*)$ van $(S,*)$, zodat $(G,*)$ een homomorf beeld is van $(K,*)$.

bewijs: Er bestaat een ondersemigroep $(S',*)$ van $(S,*)$ zodat $S'\varphi = G$.
E is de verzameling van alle idempotente elementen in S'.
Kies nu een $e \in E$, zodat $|S'*e|$ zo klein mogelijk is.
$K = e*S'*e$ is een ondersemigroep van $(S',*)$, omdat
$\forall_{s_1 \in S'} \forall_{s_2 \in S'} \exists_{s_3 \in S'} [e*s_1*e*e*s_2*e = e*(s_1*e*s_2)*e = e*s_3*e]$
e is bovendien een identiteit in $(K,*)$: $(e*s*e)*e = e*s*e*e = e*(e*s*e)$.
Stel nu: $f \in K \cap E \Rightarrow \exists_{s_1 \in S'} [f = e*s_1*e] \Rightarrow S'*f = S'*e*s_1*e \leq S'*e$
$S'*e$ is zo klein mogelijk: $|S'*e| \leq |S'*f|$ $\Rightarrow S'*e = S'*f$
$e = e*e \in S'*e = S'*f \Rightarrow \exists_{s_2 \in S'} [e = s_2*f] \Rightarrow e = s_2*f = s_2*f*f = e*f = e*e*s_1*e = e*s_1*e = f$.
e is dus het enige idempotente element van K.
Tot slot nog de inverse:
$\forall_{s \in S'} \exists_{n \geq 0} [(e*s*e)^n * (e*s*e)^n = (e*s*e)^n]$ (zie 4.3.2.)
e is echter het enige idempotente element, dus $(e*s*e)^n = e$.
Hieruit volgt dat $(e*s*e)^{n-1}$ de inverse van $e*s*e$ is.
$(K,*)$ is dus een groep.
De stelling volgt nu direkt, want
$K\varphi = (e*S'*e)\varphi = (e\varphi)*(S'\varphi)*(e\varphi) = e_G*G*e_G = G$.

4.3.5. V is een eindige verzameling.
(S,) is een semigroep van afbeeldingen van V in V.
(K,) is een ondergroep van (S,).

Er bestaat een deelverzameling W van V, zodat de restricties van de elementen van K tot W permutaties over W zijn, die een groep isomorf aan (K,) genereren.

bewijs: Stel: $W := V\varepsilon = pr_2\varepsilon$ waarbij ε de identiteit van (K,) is.
$\varepsilon\varepsilon = \varepsilon \Rightarrow \forall_{a\in V}[a\varepsilon = b \Rightarrow b\varepsilon = b] \Rightarrow D_W\varepsilon = D_W$.

$\kappa \in K$, en $\kappa\eta = \varepsilon$ (η bestaat, omdat (K,) een groep is).
Als $a \in W$ en $a\kappa = b$, dan moet $b\eta = a$ (immers $a\varepsilon = a$).
Ook geldt $\eta\kappa = \varepsilon$ en dus $b \in W$ (immers $b\eta = a$ en $a\kappa = b$) $\Rightarrow \kappa \in K \Rightarrow W\kappa \subseteq W$

Stel nu: $a \in W$, $b \in W$, $a \neq b$, $\kappa \in K$, $a\kappa = c$ en $b\kappa = c$. Dan komen we tot een tegenspraak: $\neg \exists_{\eta\in K}[\kappa\eta = \varepsilon]$ (η is immers een afbeelding) Dit is in strijd met het feit dat (K,) een groep is.
Hieruit volgt $W\kappa = W \Rightarrow D_W\kappa$ is een permutatie over W.

We definiëren nu φ met $\forall_{\kappa\in K}[\kappa\varphi = D_W\kappa]$.
φ is een isomorfisme, want
φ is een-eenduidig: $\kappa = \eta \Rightarrow D_W\kappa = D_W\eta$ (triviaal) en $D_W\kappa = D_W\eta \Rightarrow \kappa = \eta$,
omdat $\kappa = \varepsilon\kappa = \varepsilon D_W\kappa = \varepsilon D_W\eta = \varepsilon\eta = \eta$ (immers $W = pr_2\varepsilon$).
φ is een homomorfisme: $(\kappa\eta)\varphi = \kappa\varphi\eta\varphi$, omdat als $D_W\kappa D_W\eta = D_W\kappa\eta$.

4.3.6. V is een eindige verzameling.
(S,) is een semigroep van afbeeldingen van V in V.
Als er een deelverzameling W van V bestaat, zodat de restricties van sommige elementen van S permutaties over W zijn, die een groep (G,) genereren, dan (G,) | (S,).

bewijs: De elementen van S, waarvan de restricties tot W permutaties zijn, vormen de verzameling T. Daar T gesloten is voor samenstellen, is (T,) een ondersemigroep van (S,).(4.1.12.). T bevat dus een element dat idempotent is (4.3.3.). Kies dan een idempotent element ε van T, zodat $|T\varepsilon|$ zo klein mogelijk is. In het bewijs van 4.3.4. zagen we dat $(\varepsilon T\varepsilon,)$ een ondergroep van $(T\varepsilon,)$ en dus van (S,) is met ε als eenheid.

Daar ε idempotent is en $D_W\varepsilon$ een permutatie over W, moet ε alle elementen van W op zichzelf afbeelden. Dwz. alle permutaties over W, die in T voorkomen, komen ook in $\varepsilon T\varepsilon$ voor.

(K,) is nu de ondergroep van $(\varepsilon T\varepsilon,)$, die gegenereerd wordt door die elementen van $\varepsilon T\varepsilon$, die, als restrictie tot W, permutaties zijn, die in G voorkomen. (K,) is dan natuurlijk een ondergroep van (S,).
De afbeelding φ van K op G definiëren we nu zo, dat
$\forall_{\kappa\in K}[\kappa\varphi = \gamma]$ als γ dezelfde permutatie over W is.
Het is dan duidelijk dat φ een homomorfisme van (K,) op (G,) is.

5. Eindige automaten

5.1. Definities

5.1.1. Een eindig automaat bestaat uit drie eindige verzamelingen Q, X en Y en een relatie $\tau \subseteq Q \times X \times Y \times Q$.

Q noemen we de toestandsverzameling.
X noemen we de verzameling van ingangssymbolen.
Y noemen we de verzameling van responsiesymbolen.

We spreken over een toestandsovergang van $q \in Q$ naar $q' \in Q$ als gevolg van een ingangssymbool $x \in X$ en onder afgave van een responsiesymbool $y \in Y$ als $(q,x,y,q') \in \tau$.

5.1.2. A is een eindig automaat.

A heet deterministisch als $\forall_{q \in Q} \; \forall_{x \in X} \left[|\tau \cap (\{q\} \times \{x\} \times Y \times Q)| \leq 1 \right]$

A heet volledig als $\forall_{q \in Q} \; \forall_{x \in X} \left[|\tau \cap (\{q\} \times \{x\} \times Y \times Q)| \geq 1 \right]$

A is volledig en deterministisch als $\forall_{q \in Q} . \forall_{x \in X} \; \exists!_{(y,q') \in Y \times Q} [(q,x,y,q') \in \tau]$

We beperken ons voortaan tot volledige, deterministische, eindige automaten, tenzij anders vermeld. We geven zo'n automaat iha. met een hoofdletter A, eventueel voorzien van extra tekens om onderling te kunnen onderscheiden. Deze tekens komen dan ook bij de bijbehorende verzamelingen en relaties op.

5.1.3. De toestandstabel van A is een matrix met $|Q|$ rijen en $|X|$ kolommen, waarvoor geldt
$t_{ij} = q_m \iff \exists_{y_p \in Y} (q_i, x_j, y_p, q_m)$

De responsietabel van A is een matrix R met $|Q|$ rijen en $|X|$ kolommen, waarvoor geldt
$r_{ij} = y_p \iff \exists_{q_m \in Q} (q_i, x_j, y_p, q_m)$

5.1.4. A' heet een deelautomaat van A als
$(Q' \subseteq Q) \wedge (X' \subseteq X) \wedge (Y' \subseteq Y) \wedge (\tau' \subseteq \tau)$.

5.1.5. Z is een niet-lege, eindige verzameling symbolen.
Een geordende rij symbolen noemen we een symboolrij of een woord.
Z^∞ is de verzameling van eindige symboolrijen, waarvan de symbolen element zijn van Z.
De lengte van een symboolrij z, aangegeven met l(z), is het aantal symbolen dat zij bevat (herhalingen meetellen!)
Concatenatie is een afbeelding γ van $Z^\infty \times Z^\infty$ in Z^∞ .
$z_1 \in Z$, $z_2 \in Z$, dan is $\gamma(z_1, z_2)$ de symboolrij die gevormd wordt door de geordende rij symbolen van z_1 te laten voorafgaan aan de geordende rij symbolen die z_2 vormen. We geven $\gamma(z_1, z_2)$ aan met $z_1 z_2$
$l(z_1 z_2) = l(z_1) + l(z_2)$.

5.1.6. $(Z^\infty, \;)$ is een semigroep.

bewijs: Concatenatie van twee symboolrijen geeft weer een symboolrij.
Concatenatie is associatief.

5.1.7. De lege symboolrij definiëren we als de symboolrij, waarvoor geldt:
$\forall_{z \in Z^\infty} [z\Lambda = \Lambda z = z]$ en $\Lambda\Lambda = \Lambda$ en $l(\Lambda) = 0$

$Z^* = Z^\infty \cup \{\Lambda\}$
$Z^k = \{z \mid z \in Z^* \wedge l(z) = k\}$

5.1.8. $(Z^*, \ )$ is een monoïde. We noemen het het door Z gegenereerde vrije monoïde.

bewijs: Door de definitie van Λ geldt voor Z^* hetzelfde als voor Z^∞: $(Z^*, \ )$ is een semigroep.
Bovendien geldt: $\forall_{z \in Z^*} [z\Lambda = \Lambda z = z]$
Λ is dus een eenheid.

5.1.9. $\tau^* \subseteq Q \times X^* \times (Y \cup \{\Lambda\}) \times Q$ wordt recursief als volgt gedefinieerd:
$\tau \cup \{(q, \Lambda, \Lambda, q) \mid q \in Q\} \subseteq \tau^*$
$\forall_{q,q',q'' \in Q} \ \forall_{w,w' \in X^*} \ \forall_{y,y' \in Y \cup \{\Lambda\}} [(q,w,y,q') \in \tau^* \wedge (q',w',y',q'') \in \tau^* \Rightarrow (q,ww',y',q'') \in \tau^*]$

5.1.10. Voor $w \in X^*$ definiëren we $\tau_w \subseteq Q \times Q$:
$\forall_{q_1 \in Q} \ \forall_{q_2 \in Q} [(q_1, q_2) \in \tau_w \Leftrightarrow \exists_{y \in Y \cup \{\Lambda\}} [(q_1, w, y, q_2) \in \tau^*]]$

5.1.11. Voor $w \in X^*$ definiëren we $\sigma_w \subseteq Q \times (Y \cup \{\Lambda\})$
$\forall_{q_1 \in Q} \ \forall_{y \in Y \cup \{\Lambda\}} [(q_1, y) \in \sigma_w \Leftrightarrow \exists_{q_2 \in Q} [(q_1, w, y, q_2) \in \tau^*]]$

5.1.12. τ_w en σ_w zijn afbeeldingen van Q in Q resp. van Q in $Y \cup \{\Lambda\}$.

bewijs: De stelling is een direkt gevolg van het feit dat we slechts deterministische en volledige automaten beschouwen.

5.2. Toestandsautomaten

5.2.1. De toestandsautomaat $\mathcal{A}$ van A is de relationaalstructuur $(Q; \{\tau_x \mid x \in X\})$.

5.2.2. De verzameling relaties $\{\tau_w \mid w \in X^*\}$ met produktvorming als bewerking is een eindig monoïde $(S_A, \ )$

bewijs: Uit 5.1.9. en 5.1.10. volgt:
$\forall_{w_1 \in X^*} \ \forall_{w_2 \in X^*} [(q_1, q_2) \in \tau_{w_1} \wedge (q_2, q_3) \in \tau_{w_2} \Rightarrow (q_1, q_3) \in \tau_{w_1 w_2}]$
dwz. $\tau_{w_1} \tau_{w_2} = \tau_{w_1 w_2}$
Relatievermenigvuldiging is associatief (2.3.2.)
Bovendien is de identiteit D_Q aanwezig: $\tau_\Lambda = \{(q,q) \mid q \in Q\}$
De relaties zijn afbeeldingen (5.1.12.). Q is een eindige verzameling (5.1.1.). Er zijn dus slechts $|Q|^{|Q|}$ afbeeldingen van Q in Q mogelijk.

5.2.3. Het monoïde $(S_A, \ )$ noemen we de semigroep van A.

5.2.4. De afbeelding $\varphi \subseteq X^* \times S_A$ met
$\forall_{w \in X^*} [w\varphi = \tau_w]$
is een homomorfisme en dus is $\varphi\varphi^{-1}$ een congruentierelatie over X^*.

bewijs: $w_1\varphi \ w_2\varphi = \tau_{w_1} \tau_{w_2} = \tau_{w_1 w_2} = w_1 w_2 \varphi$.
De rest volgt uit 3.3.5. en 2.5.6.

5.2.5. Als een eindig monoïde (M,) gegeven is, dan kunnen we een toestandsautomaat $\mathcal{A}$ construeren, zodat $(S_{\mathcal{A}},)$ isomorf is met (M,).

bewijs: $X \subseteq M$, zodat $\langle X \rangle = M$ (men mag ook X=M nemen)
$Q = M$
$\tau_x = \{(m_1, m_2) \mid m_2 = m_1 x\}$

Elke $m \in M$ is te schrijven als het produkt van elementen van X, omdat $\langle X \rangle = M$.
Stel nu: $m = x_1 x_2 \ldots x_k = v$.
We definiëren hiermee een afbeelding $\varphi \subseteq M \times S_{\mathcal{A}}$:
$m\varphi = \tau_v$.

φ is een-eenduidig, want als $m_1 \neq m_2$, dan $\tau_{v_1} \neq \tau_{v_2}$ met $m_1 = v_1$, $m_2 = v_2$.
immers $e\tau_{v_1} = em_1 = m_1$ en $e\tau_{v_2} = em_2 = m_2$.
φ is ook een homomorfisme, want $(m_1 m_2)\varphi = \tau_{v_1 v_2} = \tau_{v_1}\tau_{v_2} = m_1\varphi\ m_2\varphi$.

5.2.6. Als een congruentierelatie R met eindige index over X^* gegeven is, dan kunnen we een toestandsautomaat $\mathcal{A}$ construeren, zodat $R = \varphi\varphi^{-1}$.

bewijs: De toestanden van $\mathcal{A}$ zijn de congruentieklassen van R . X is de verzameling ingangssymbolen.
$\tau_x = \{([v]_R, [vx]_R) \mid v \in X^*\}$
Deze definitie is correct, omdat R een congruentierelatie is: $vRw \Rightarrow (vx)R(wx)$.

opm. Blijkbaar hoeft R slechts rechtscongruent te zijn. Dan reeds kunnen we een bijbehorende $\mathcal{A}$ construeren. Een dergelijk toestandsautomaat heeft een speciale eigenschap: $[\Lambda]_R \tau_w = [w]_R$. Elke toestand is vanuit $[\Lambda]_R$ te bereiken.

5.2.7. Een toestandsautomaat met een toestand q_0 van waaruit elke andere toestand te bereiken is, heet cyclisch. q_0 heet de begintoestand.

5.2.8. Een toestandsautomaat $\mathcal{A}'$ heet een deeltoestandsautomaat van $\mathcal{A}$ als
$(Q' \subseteq Q) \wedge (X' \subseteq X) \wedge \forall_{x \in X'} [\tau'_x \subseteq \tau_x]$

5.2.9. Als $\mathcal{A}'$ een deeltoestandsautomaat is van $\mathcal{A}$, dan $(S_{\mathcal{A}'},) \mid (S_{\mathcal{A}},)$.

bewijs: $S = \langle \{\tau_w \mid w = \Lambda \vee w \in X'\} \rangle$
$(S,)$ is een ondersemigroep van $(S_{\mathcal{A}},)$
$S_{\mathcal{A}'} = (\{D_{Q'}\tau_w \mid \tau_w \in S\},)$
We definiëren nu de afbeelding φ van S op $S_{\mathcal{A}'}$ als volgt: $\tau_w\varphi = D_{Q'}\tau_w$
φ is een homomorfisme, want $(\tau_v \tau_w)\varphi = D_{Q'}\tau_v\tau_w = D_{Q'}\tau_v\, D_{Q'}\tau_w = \tau_w\varphi\ \tau_v\varphi$

5.2.10. Voor twee toestandsautomaten $\mathcal{A}$ en $\mathcal{A}'$ kan gelden:
Er bestaat een afbeelding φ van Q op Q' en een afbeelding η van X op X' zodat:
$\forall_{x \in X} [\tau_x \varphi = \varphi \tau'_{x\eta}]$
In zo'n geval heet $\mathcal{A}'$ een homomorf beeld van $\mathcal{A}$.

opm. Dit is geen homomorfisme in de zin van 2.5.2.. In de meeste gevallen zal η een-eenduidig zijn en dan is alles in overeenstemming met 2.5.2.:
Voor φ kiest men dan φ en Ψ definieert men zodanig, dat $\Psi(\tau_x) = \tau'_{x\eta}$
Voor η kan men dan net zo goed de identiteit kiezen.

Als φ ook een-eenduidig is, dan noemen we $\mathcal{A}$ en $\mathcal{A}'$ isomorf.

5.2.11. Een partitie μ van Q noemen we een toelaatbare partitie van $\mathcal{A}$ als
$\forall_{x\in X}\ \forall_{B_i\in\mu}\ \exists_{B_j\in\mu}[B_i\tau_x \subseteq B_j]$

5.2.12. μ is een toelaatbare partitie van $\mathcal{A}$.
We definiëren nu een toestandsautomaat $\mathcal{A}'$:
$X'=X$, $Q'=\mu$ en $\underline{B}_i\tau_x=\underline{B}_j \Leftrightarrow B_i\tau_x \subseteq B_j$.
Dan is $\mathcal{A}'$ een homomorf beeld van $\mathcal{A}$.
We geven het aldus gedefinieerde toestandsautomaat vaak aan met $\mathcal{A}/\mu$.

bewijs: η is de identiteit en voor φ laten we gelden:
$\forall_{q\in Q}\ [q\varphi=\underline{B}_i \Leftrightarrow q\in B_i]$
Dan voor alle $q\in B_j$
$q\tau_x\varphi=q'\varphi=\underline{B}_j=\underline{B}_i\tau_x'$ en $q\varphi\tau_x'=\underline{B}_i\tau_x'$ Dus $\tau_x\varphi=\varphi\tau_x'$

5.2.13. Als $\mathcal{A}'$ het homomorfe beeld van $\mathcal{A}$ is, dan induceert de relatie $\varphi\varphi^{-1}$ een toelaatbare partitie μ van Q.

bewijs: $q_1\equiv q_2\ (\mu) \Leftrightarrow q_1\in B \wedge q_2\in B \Leftrightarrow q_1\varphi=q_2\varphi=\underline{B}$.
$q_1\tau_x\varphi=q_1\varphi\tau_{x\eta}'=q_2\varphi\tau_{x\eta}'=q_2\tau_x\varphi$
dwz. $q_1\tau_x\equiv q_2\tau_x\ (\mu) \Rightarrow \mu$ is toelaatbaar. ○

5.2.14. Als $\mathcal{A}'$ een homomorf beeld van $\mathcal{A}$ is, dan is $(S_{A'},\ )$ een homomorf beeld van $(S_A,\ )$.

bewijs: $w\in X^*$ en $w=x_1x_2\cdots x_{l(w)}$.
$\tau_w\varphi=\tau_{x_1}\tau_{x_2}\cdots\tau_{l(w)}\varphi=\tau_{x_1}\tau_{x_2}\cdots\tau_{l(w)-1}\varphi(\tau'_{x_{l(w)}\eta})$
Zo voortgaande vindt men
$\tau_w\varphi=\varphi(\tau'_{x_1\eta})(\tau'_{x_2\eta})\cdots(\tau'_{x_{l(w)}\eta})=\varphi\prod_{i=1}^{l(w)}(\tau'_{x_i\eta})$
$\varphi^{-1}\tau_w\varphi=\varphi'\prod_{i=1}^{l(w)}(\tau'_{x_i\eta})=\prod_{i=1}^{l(w)}(\tau'_{x_i\eta})$
We definiëren de relatie ξ tussen S_A en $S_{A'}$ door: $\tau_w\xi=\prod_{i=1}^{l(w)}(\tau'_{x_i\eta})$

$v\in X^*$ en $v=z_1z_2\cdots z_{l(v)}$.
$\tau_w=\tau_v \Rightarrow \varphi^{-1}\tau_w\varphi=\varphi^{-1}\tau_v\varphi \Rightarrow \tau_w\xi=\tau_v\xi$
dwz. ξ is een afbeelding van S_A in $S_{A'}$.
Daar η X op X' afbeeldt zal elk element van $S_{A'}$ gelijk zijn aan een $\prod_{i=1}^{l(w)}(\tau'_{x_i\eta})$ voor een $w\in X^*$. ξ is surjectief.

Ten slotte:
$\forall_{v\in X^*}\ \forall_{w\in X^*}\ [\tau_v\tau_w\xi=\tau_{vw}\xi=\prod_{i=1}^{l(v)}(\tau'_{z_i\eta})\cdot\prod_{i=1}^{l(w)}(\tau'_{x_i\eta})=\tau_v\xi\,\tau_w\xi]$
ξ is dus een homomorfisme van S_A op $S_{A'}$.

opm. ξ kan een isomorfisme zijn zonder dat $\mathcal{A}$ en $\mathcal{A}'$ isomorf zijn!

5.3. Equivalentie

5.3.1. A en A' zijn twee automaten.
$X=X'$ en $Y=Y'$.
$q\in Q$ en $q'\in Q'$ heten equivalent als
$\forall_{w\in X^*}\ [(q,y)\in\sigma_w \Leftrightarrow (q',y)\in\sigma_w']$
Notatie: $q\sim q'$.

opm. De zojuist gedefinieerde relatie is een equivalentie relatie.

5.3.2. A en A' heten equivalent als
$\forall_{q\in Q}\ \exists_{q'\in Q'}[q\sim q'] \wedge \forall_{q'\in Q'}\ \exists_{q\in Q}[q'\sim q]$
Notatie: $A\sim A'$

opm. De zojuist gedefinieerde relatie is een equivalentierelatie.

5.3.3. Een automaat heet een toestand-responsie-automaat als er een afbeelding χ bestaat waarvoor geldt:
$\forall_{q\in Q}\ \forall_{x\in X}\ \big[\ (q,y)\in \sigma_x \wedge (q,q')\in \tau_x \Rightarrow (q',y)\in \chi\big]$.

5.3.4. Elk automaat heeft een equivalent toestand-responsie-automaat.

bewijs: We construeren bij een gegeven A op de volgende manier een A'.
$X=X'$ en $Y=Y'$
$Q'=\{(q,y)\mid \exists_{q'\in Q}\ \exists_{x\in X}\ [(q',x,y,q)\in\tau]\}$
$\tau'=\{((q,y),x,y',(q',y'))\mid (q,x,y,q')\in\tau\}$.

Steeds geldt: $q\sim(q,y)$.

5.3.5. A heet gereduceerd als
$\forall_{q\in Q}\forall_{q'\in Q}[q\sim q'\Rightarrow q=q']$

5.3.6. Elk automaat is equivalent aan een gereduceerd automaat.

bewijs: Volgens 5.3.4. is er een toestand-responsie-automaat A", zodat $A\sim A"$.
We moeten dus slechts bewijzen dat A" equivalent is aan een gereduceerd automaat A' (transitiviteit van $\sim$)

Q' is de verzameling equivalentieklassen over Q", dwz. $q_1''\sim q_2''\Leftrightarrow [q_1'']=[q_2'']$.
$(q_1'',x,q_2''\chi,q_2'')\in\tau''\Rightarrow([q_1''],x,[q_2'']\chi,[q_2''])\in\tau'$
(χ in het laatste lid is intuïtief ingevoerd)

We moeten nu bewijzen dat: $q_1''\sim q_2''\Rightarrow\forall_{x\in X}\big[[\tau_x''(q_1'')]=[\tau_x''(q_2'')]\big]$.
$q_1''\sim q_2''\Rightarrow \chi(q_1'')=\chi(q_2'')$.

Uit 5.3.1.: $\forall_{w\in X^*}\big[q_1''\sim q_2''\Rightarrow \sigma_w(q_1'')=\sigma_w(q_2'')\big]$
Stel nu $w=\Lambda$: $\sigma_\Lambda(q_1'')=\chi(\tau_\Lambda(q_1''))=\chi(q_1'')$
$\sigma_\Lambda(q_2'')=\chi(\tau_\Lambda(q_2''))=\chi(q_2'')$
$\Big\}\Rightarrow \chi(q'')=\chi(q'')$

$\forall_{x\in X}\ \big[\ \sigma_w(\tau_x(q_1''))=\sigma_{xw}(q_1'')=\sigma_{xw}(q_2'')=\sigma_w(\tau_x(q_2''))\Rightarrow \tau_x(q_1'')\sim\tau_x(q_2'')\Rightarrow$
$\Rightarrow[\chi(q_1'')]=[\tau_x(q_2'')]\big]$

5.3.7. q en q' heten k-equivalent als geldt
$\forall_{w\in X^*}\big[l(w)\le k\Rightarrow((q,y)\in\sigma_w\iff(q',y)\in\sigma_w)\big]$
Notatie: $q\sim_k q'$

5.3.8. Als μ_k de partitie van Q is, die bestaat uit de blokken van k-equivalente toestanden, dan voldoet de rij $\mu_0,\mu_1,\mu_2,\ldots$ aan 3.1.5.

bewijs: Dat $\sim_k$ een equivalentierelatie is en dat $\mu_{k+1}\le\mu_k$ is triviaal.
Stel daarom $\mu_k=\mu_{k+1}$:
$\forall_{x\in X}[\,q\sim_{k+1}q'\Rightarrow \tau_x(q)\sim_k\tau_x(q')]$;
daar echter $\mu_k=\mu_{k+1}$ geldt ook
$\forall_{x\in X}[\tau_x(q)\sim_{k+1}\tau_x(q')]$
Dus ook $\mu_{k+1}=\mu_{k+2}$.
De rest volgt uit in inductie.

5.3.9. Twee toestanden zijn equivalent slals ze K-equivalent zijn met $K<|Q|$.

bewijs: 3.1.5. en 5.3.8.

5.3.10. Een automaat is equivalent aan precies één gereduceerd automaat.

bewijs: Als dit niet zo zou zijn, dan zouden er twee verschillende partities $\sim_K$ zijn; dat kan niet!

5.4. Homomorfismen

5.4.1. A en A' zijn twee automaten.
φ is een afbeelding van Q in Q',
η is een afbeelding van X in X',
ϑ is een afbeelding van Y in Y'.

$(\varphi, \eta, \vartheta)$ heet een QXY-homomorfisme van A in A' als
$\forall_{q_1 \in Q} \forall_{q_2 \in Q} \forall_{x \in X} \forall_{y \in Y} [(q_1, x, y, q_2) \in \tau \Rightarrow (q_1\varphi, x\eta, y\vartheta, q_2\varphi) \in \tau']$.

5.4.2. Een QXY-homomorfisme van A in A' is een QXY-homomorfisme van A op A' als φ, η en ϑ surjectief zijn.

5.4.3. Een QXY-homomorfisme van A in A' is een isomorfisme van A op A' als φ, η en ϑ bijectief zijn en $(\varphi^{-1}, \eta^{-1}, \vartheta^{-1})$ een Q'X'Y'-homomorfisme van A' in A is.

5.4.4. Een QXY-homomorfisme van A op A' noemen we een homomorfisme van A op A' als $(X=X') \wedge (Y=Y') \wedge (\eta = D_X) \wedge (\vartheta = D_Y)$

5.4.5. $\Psi \subseteq Q \times Q'$, $pr_1 \Psi = Q$ en $pr_2 \Psi = Q'$.
$\forall_{x \in X} [\Psi^{-1} \tau_x \subseteq \tau_x' \Psi^{-1}]$
$\forall_{x \in X} [\Psi^{-1} \sigma_x \subseteq \sigma_x']$
Dan noemen we Ψ een zwak homomorfisme van A op A'.

5.4.6. φ is een afbeelding van Q op Q'.
(φ, D_X, D_Y) is een homomorfisme slals
$\forall_{x \in X} [\tau_x \varphi = \varphi \tau_x']$
$\forall_{x \in X} [\sigma_x = \varphi \sigma_x']$

bewijs: Zij (φ, D_X, D_Y) een homomorfisme van A op A'.
$(q_1, x, y, q_2) \in \tau \Rightarrow (q_1, q_2\varphi) \in \tau_x\varphi \wedge (q_1, y) \in \sigma_x$.
5.4.1. $\Rightarrow (q_1\varphi, x, y, q_2\varphi) \in \tau' \Rightarrow (q_1, q_2\varphi) \in \varphi\tau_x' \wedge (q_1\varphi, y) \in \sigma_x'$.
Voor volledige, deterministische automaten zijn τ_x en σ_x afbeeldingen, dus $\tau_x\varphi = \varphi\tau_x'$ en $\sigma_x = \varphi\sigma_x'$.

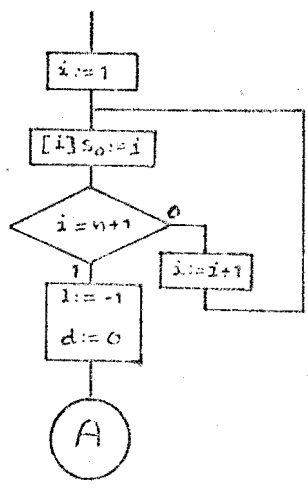
Stel nu $\tau_x\varphi = \varphi\tau_x'$ en $\sigma_x = \varphi\sigma_x'$ voor alle $x \in X$, dan
$(q_1, q_2) \in \tau_x \Rightarrow (q_1, q_2\varphi) \in \tau_x\varphi \Rightarrow (q_1, q_2\varphi) \in \varphi\tau_x' \Rightarrow \exists_{q' \in Q'} [q_1\varphi = q' \wedge (q', q_2\varphi) \in \tau_x'] \Rightarrow (q_1\varphi, q_2\varphi) \in \tau_x'$
$(q_1, y) \in \sigma_x \Rightarrow \exists_{q' \in Q'} [q_1\varphi = q' \wedge (q', y) \in \sigma_x'] \Rightarrow (q_1\varphi, y) \in \sigma_x'$
Hieruit volgt: $(q_1, x, y, q_2) \in \tau \Rightarrow (q_1\varphi, x, y, q_2\varphi) \in \tau'$. Bovendien was gegeven dat φ surjectief was, dus (φ, D_X, D_Y) is een homomorfisme van A op A'.

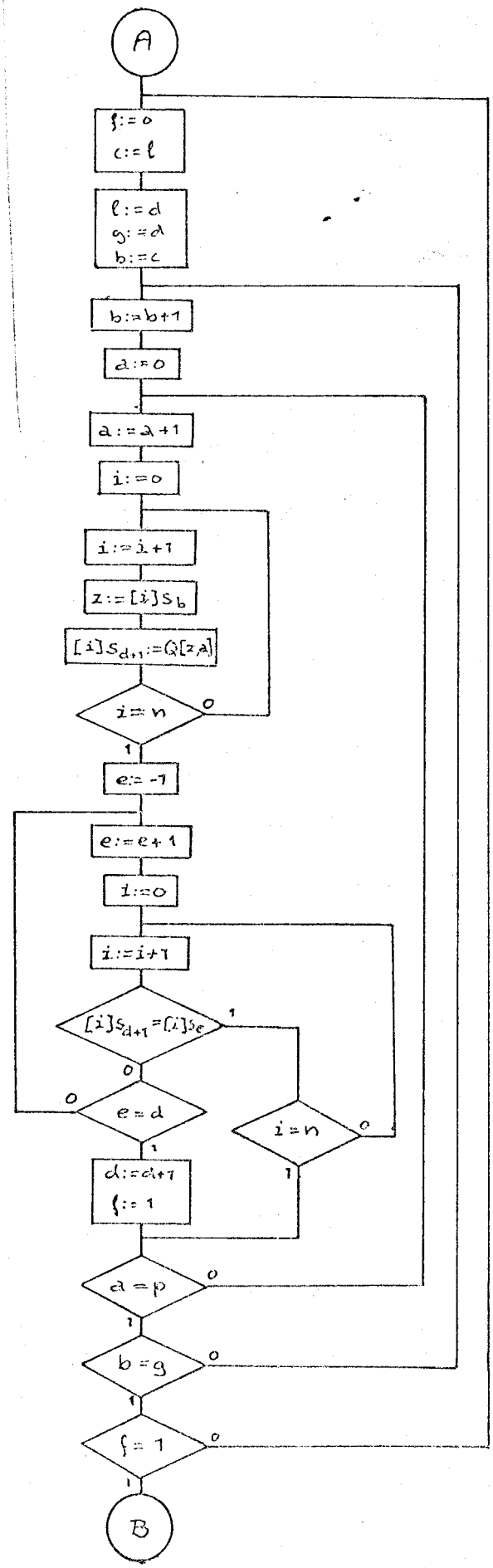
5.4.7. φ is een afbeelding van Q in Q'.
(φ, D_X, D_Y) is een homomorfisme van A op A' slals φ een zwak homomorfisme is van A op A.

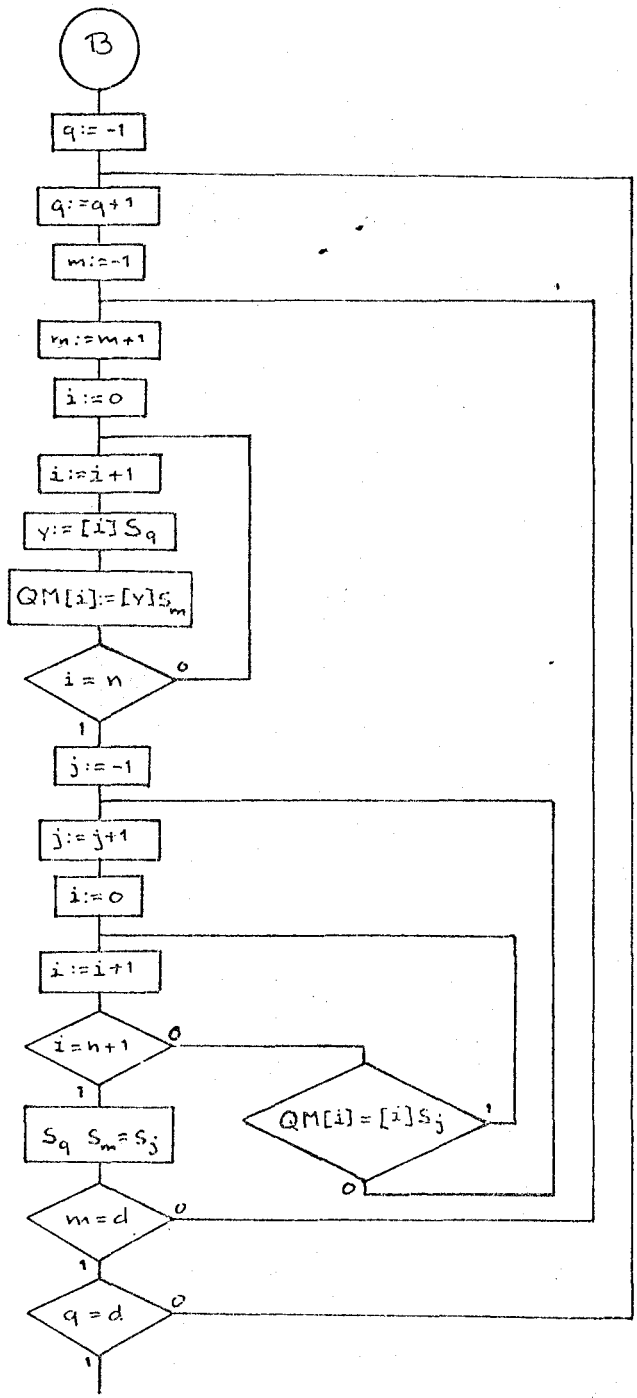
bewijs: (ς, D_X, D_Y) een homomorfisme $\Rightarrow$ ς is een surjectieve afbeelding $\Rightarrow$
$\Rightarrow$ $pr_1 \varsigma = Q \wedge pr_2 \varsigma = Q'$.

Volgens 5.4.5. geldt voor willekeurige $x \in X$
$\varsigma^{-1} \tau_x \varsigma = \tau_x' \Rightarrow \varsigma^{-1} \tau_x \varsigma \varsigma^{-1} = \tau_x' \varsigma^{-1} \Rightarrow \varsigma^{-1} \tau_x D_Q \subseteq \tau_x' \varsigma^{-1} \Rightarrow \varsigma^{-1} \tau_x \subseteq \tau_x' \varsigma^{-1}$.
Ook $\varsigma^{-1} \sigma_x \subseteq \sigma_x'$.
Dwz ς is een zwak homomorfisme van A op A'.

Stel nu: ς is een zwak homomorfisme van A op A'
Dan $pr_2 \varsigma = Q'$, dus ς is surjectief.
Bovendien geldt voor alle $x \in X$:
$\varsigma^{-1} \tau_x = \tau_x' \varsigma^{-1} \Rightarrow \varsigma \varsigma^{-1} \tau_x \varsigma = \varsigma \tau_x' \varsigma^{-1} \varsigma \Rightarrow D_Q \tau_x \varsigma = \varsigma \tau_x' D_{Q'} \Rightarrow \tau_x \varsigma = \varsigma \tau_x'$.
$\varsigma^{-1} \sigma_x = \sigma_x' \Rightarrow \varsigma \varsigma^{-1} \sigma_x = \varsigma \sigma_x' \Rightarrow D_Q \sigma_x = \varsigma \sigma_x' \Rightarrow \sigma_x = \varsigma \sigma_x'$.
De =-tekens zijn toegestaan, omdat ς een afbeelding is!




A
f:=0
c:=l
l:=d
g:=d
b:=c
b:=b+1
a:=0
a:=a+1
i:=0
i:=i+1
z:=[i]s_b
[i]s_d+1:=Q[z,A]
i=n
0
1
e:=-1
e:=e+1
i:=0
i:=i+1
[i]s_d+1=[i]s_e
1
0
e=d
0
i=n
0
1
d:=d+1
f:=1
a=p
0
1
b=g
0
1
f=1
0
1
B


B
q:= -1
q:=q+1
m:=-1
m:=m+1
i:=0
i:=i+1
y:=[i]Sq
QM[i]:=[y]Sm
i = n
0
1
j:=-1
j:=j+1
i:=0
i:=i+1
i=n+1
0
1
Sq Sm=Sj
QM[i] = [i]Sj
1
0
m=d
0
1
q=d
0
1

6. Realisatie

6.1. Definitie en eigenschappen

6.1.1. A en A' zijn twee automaten.
X=X' en Y=Y'.
Bestaat er een afbeelding κ van Q in Q' zodat
$\forall_{w\in X^*}\,[\tau'_w = \kappa\tau_w]$
dan wordt A door A' gerealiseerd.
Notatie: $A' \geq A$.

Is λ een afbeelding van een deelverzameling van Q' op Q en geldt
$\forall_{x\in X}\,[\lambda\tau_x \subseteq \tau'_x\lambda]$
dan wordt $\mathcal{A}$ door $\mathcal{A}'$ gerealiseerd.
Notatie: $\mathcal{A}' \geq \mathcal{A}$.

6.1.2. Als $\mathcal{A}' \geq \mathcal{A}$ en $pr_1\,\lambda = P \subseteq Q'$, dan
$\forall_{x\in X}\;[\lambda\tau_x = D_P\tau'_x\lambda]$

6.1.3. Natuurlijk is het algemener in de definitie van realiseren ook een afbeelding van X in X' op te nemen ipv. X=X' te stellen. Dit is echter niet essentieel.

Veronderstel bv. dat het laatste gedeelte van 6.1.1. als volgt luidt:
Is λ een afbeelding van een deelverzameling van Q' op Q en ξ een afbeelding van X in X', zodat
$\forall_{x\in X}\;[\lambda\tau_x \subseteq \tau'_{x\xi}\lambda]$
dan wordt $\mathcal{A}$ door $\mathcal{A}'$ gerealiseerd.
Notatie: $\mathcal{A}' \geq \mathcal{A}$.

We gaan er nu vanuit dat $\mathcal{A}' \geq \mathcal{A}$:
$\left.\begin{array}{l} \tau_{x_1} \neq \tau_{x_2} \Rightarrow \exists_{q\in Q}\,[q\tau_{x_1} \neq q\tau_{x_2}] \\ \lambda \text{ is surjectief} \Rightarrow \exists_{q'\in Q}\,[q'\lambda = q] \end{array}\right\} \Rightarrow q'\lambda\tau_{x_1} = q\tau_{x_1} \neq q\tau_{x_2} = q'\lambda\tau_{x_2} \Rightarrow \tau'_{x_1\xi} \neq \tau'_{x_2\xi}$
Als nu $\tau'_{x_1\xi} = \tau'_{x_2\xi}$, dan moet $q'\tau'_{x_1\xi}\lambda = q'\tau'_{x_2\xi}\lambda$; dwz. dat niet x_1 en x_2 beide aan de eis van de nieuwe definitie kunnen voldoen.

Conclusie: Als $\forall_{x_1\in X}\,\forall_{x_2\in X}\,[\,x_1 \neq x_2 \Rightarrow \tau_{x_1} \neq \tau_{x_2}]$, dan moet ξ een-eenduidig zijn en dan is zijn effect slechts andere namen geven aan de ingangssymbolen.

6.1.4. $\forall_{x\in X}\,[\lambda\tau_x \subseteq \tau'_x\lambda] \Rightarrow \forall_{w\in X^*}\,[\lambda\tau_w \subseteq \tau'_w\lambda]$

6.1.5. $A \geq A' \wedge A' \geq A \Rightarrow A \sim A'$

bewijs: Uit $A \geq A'$ volgt:
$\left.\begin{array}{l} \forall_{w\in X^*}\,[\tau'_w = \kappa\tau_w] \\ \forall_{q'\in Q'}\,\exists_{q\in Q}\,[q = q'\kappa] \end{array}\right\} \Rightarrow \forall_{q'\in Q'}\,\exists_{q\in Q}\,[q \sim q']$.
Zo volgt ook uit $A' \geq A$: $\forall_{q\in Q}\,\exists_{q'\in Q'}\,[q \sim q']$.
Volgens 5.1.3. geldt dan $A \sim A'$.

6.1.6. X=X' en Y=Y'.
(ζ, D_X, D_Y) is een isomorfisme van A op een deelautomaat van A'.
Dan $A' \geq A$ en $\mathcal{A}' \geq \mathcal{A}$.

bewijs: Kies $\kappa = \zeta$ en $\lambda = \zeta^{-1}$.

6.1.7. $(A' \geq A) \wedge (A'' \geq A') \Rightarrow (A'' \geq A)$

6.1.8. $(\mathcal{A}' \geq \mathcal{A}) \wedge (\mathcal{A}'' \geq \mathcal{A}') \Rightarrow (\mathcal{A}'' \geq \mathcal{A})$

bewijs: Er bestaan afbeeldingen λ en λ', zodat
$\forall_{x \in X} \left[(\lambda \tau_x \leq \tau_x' \lambda) \wedge (\lambda' \tau_x' \leq \tau_x'' \lambda') \right]$
We definiëren nu $\lambda'' = \lambda' \lambda$ (dit is een afbeelding uit Q'' op Q).
Dan geldt:

$$\forall_{q_1'' \in Q''} \; \forall_{q_1 \in Q} \; \forall_{x \in X} \left[(q_1'', q_1) \in \lambda'' \tau_x \Rightarrow \right.$$
$$\Rightarrow \exists_{q_2 \in Q} \left[q_1'' \lambda'' = q_2 \wedge q_2 \tau_x = q_1 \right] \Rightarrow$$
$$\Rightarrow \exists_{q_1' \in Q'} \left[q_1'' \lambda' = q_1' \wedge q_1' \lambda = q_2 \wedge q_2 \tau_x = q_1 \right] \Rightarrow$$
$$\Rightarrow \exists_{q_2' \in Q'} \left[q_1'' \lambda' = q_1' \wedge q_1' \tau_x' = q_2' \wedge q_2' \lambda = q_1 \right] \Rightarrow$$
$$\Rightarrow \exists_{q_2'' \in Q''} \left[q_1'' \tau_x'' = q_2'' \wedge q_2'' \lambda' = q_2' \wedge q_2' \lambda = q_1 \right] \Rightarrow$$
$$\left. \Rightarrow (q'', q) \in \tau_x'' \lambda'' \right]$$

dwz. $\tau_x'' \lambda'' \geq \lambda'' \tau_x$.
Dus $\mathcal{A}'' \geq \mathcal{A}$.

6.1.9. Als $\mathcal{A}' \geq \mathcal{A}$, dan bestaat er een A'', zodat $\mathcal{A}'' = \mathcal{A}' \wedge A'' \geq A$.

bewijs: Er bestaat een afbeelding λ uit Q' op Q, waarvoor geldt:
$\forall_{x \in X} \left[\lambda \tau_x \leq \tau_x' \lambda \right]$

Neem een willekeurige $y_0 \in Y$.
$\tau'' \subseteq Q' \times X \times Y \times Q'$ maken we zo, dat voor alle $x \in X$

$$\tau_x'' = \tau_x' \wedge \forall_{q' \in Q'} \left[q' \sigma_x'' = \begin{cases} q' \lambda \sigma_x & \text{als } \{q'\} \lambda \sigma_x \neq \emptyset \\ y_0 & \text{als } \{q'\} \lambda \sigma_x = \emptyset \end{cases} \right]$$

Hiermee is een volledig, deterministiesch automaat gedefinieerd, waarvoor geldt: $\mathcal{A}'' = \mathcal{A}'$
$\forall_{x \in X} \left[\lambda \sigma_x \leq \sigma_x'' \right]$

Omdat λ een afbeelding op Q is, bestaat er een afbeelding κ van Q in Q' met $\kappa \subseteq \lambda^{-1}$.
Stel nu: $w = x_1 x_2 \ldots x_k \in X^*$, dan

$$\kappa^{-1} \sigma_w \leq \lambda \sigma_w = \lambda \tau_{x_1 x_2 \ldots x_{k-1}} \sigma_{x_k} \leq \tau'_{x_1 x_2 \ldots x_{k-1}} \lambda \sigma_{x_k} = \tau''_{x_1 x_2 \ldots x_{k-1}} \lambda \sigma_{x_k} = \sigma_w'' \Rightarrow$$
$$\Rightarrow \sigma_w \leq \kappa \kappa^{-1} \sigma_w \leq \kappa \sigma_w''$$

Dus
$\sigma_w \leq \kappa \sigma_w''$
σ_w is een afbeelding met $\mathrm{pr}_1 \sigma_w = Q$
$\kappa \sigma_w''$ is een afbeelding met $\mathrm{pr}_1 \kappa \sigma_w'' = Q$
$\Rightarrow \sigma_w = \kappa \sigma_w''$
Dit betekent: $A'' \geq A$.

6.1.10. Als er een zwak homomorfisme van A op A' bestaat, dan $A' \geq A$.

bewijs: $w = x_1 x_2 \ldots x_k \in X^*$.

$$\psi^{-1} \sigma_w = \psi^{-1} \tau_{x_1 x_2 \ldots x_{k-1}} \sigma_{x_k} \leq \tau'_{x_1} \psi^{-1} \tau_{x_2 x_3 \ldots x_{k-1}} \sigma_{x_k} \leq \ldots \ldots \leq \tau'_{x_1 x_2 \ldots x_{k-1}} \psi^{-1} \sigma_{x_k} \leq$$
$$\leq \tau'_{x_1 x_2 \ldots x_{k-1}} \sigma'_{x_k} = \sigma'_w$$

Daar $\mathrm{pr}_1 \psi = Q_1$ is er ook een afbeelding κ van Q in Q', zodat $\kappa \leq \psi^{-1}$.

$$\kappa^{-1} \sigma_w \leq \psi^{-1} \sigma_w \leq \sigma_w' \Rightarrow \sigma_w = I_Q \sigma_w \leq \kappa \kappa^{-1} \sigma_w \leq \kappa \sigma_w'$$

dwz. $A' \geq A$.

6.1.11. Als A een gereduceerd automaat is en $A' \geq A$, dan $\mathcal{A}' \geq \mathcal{A}$.

bewijs: Er bestaat een afbeelding van Q in Q', zodat
$\forall_{w \in X^*} [\sigma_w = \kappa \sigma_w']$.
We definiëren λ als
$\lambda := \bigcup_{w \in X^*} (\kappa \tau_w')^{-1} \tau_w$
Dan $\kappa^{-1} = (\kappa \tau_\Lambda')^{-1} \tau_\Lambda \subseteq \lambda \Rightarrow Q = pr_1 \kappa^{-1} \subseteq pr_2 \lambda$
$pr_2 \lambda \subseteq Q$ $\Rightarrow pr_2 \lambda = Q$.

Volgens 2.3.5.
$\forall_{w \in X^*} [(\kappa \tau_w')^{-1} \kappa \tau_w' \subseteq D_{Q'}]$
Dit gebruiken we in de volgende regel:
$\forall_{v \in X^*} [\lambda \sigma_v = \bigcup_{w \in X^*} (\kappa \tau_w')^{-1} \tau_w \sigma_v = \bigcup_{w \in X^*} (\kappa \tau_w')^{-1} \sigma_{wv} \subseteq \bigcup_{w \in X^*} (\kappa \tau_w')^{-1} \kappa \sigma_w' =$
$= \bigcup_{w \in X^*} (\kappa \tau_w')^{-1} \kappa \tau_w' \sigma_v \subseteq D_{Q'} \sigma_v' = \sigma_v']$
Stel nu $q' \in \bigcup_{w \in X^*} pr_1 \tau_w' \Rightarrow q' \in pr_1 \lambda$ en $\{q_1, q_2\} \subseteq \{q'\} \lambda$, dan
$\forall_{w \in X^*} [\{q_1, q_2\} \sigma_w \subseteq \{q'\} \lambda \sigma_w \subseteq \{q'\} \sigma_w'] \Rightarrow \forall_{w \in X^*} [q_1 \sigma_w = q_2 \sigma_w] \Rightarrow q_1 = q_2$
immers A is gereduceerd.
Hieruit zien we dat λ een afbeelding van een deelverzameling van Q' op Q is.

Voor willekeurige $x \in X$ geldt nu:
$\forall_{q' \in Q'} [\{q'\} \lambda \tau_x \neq \emptyset \Rightarrow \{q'\} \lambda \tau_x = \{q'\} (\bigcup_{w \in X^*} (\kappa \tau_w')^{-1} \tau_w) \tau_x \subseteq$
$\subseteq \{q'\} \tau_x' (\tau_x')^{-1} (\bigcup_{w \in X^*} (\kappa \tau_w')^{-1} \tau_w) \tau_x =$
$= \{q'\} \tau_x' (\bigcup_{w \in X^*} (\kappa \tau_{wx}')^{-1} \tau_{wx}) \subseteq \{q'\} \tau_x' \lambda]$
Dit betekent dat $\lambda \tau_x \subseteq \tau_x' \lambda$
Dus $\mathcal{A}' \geq \mathcal{A}$

6.1.12. $\mathcal{A}' \geq \mathcal{A}$ slals $\mathcal{A}$ een homomorf beeld van een deeltoestandsautomaat van $\mathcal{A}'$ is.

bewijs: Als $\mathcal{A}' \geq \mathcal{A}$, dan is er een afbeelding λ van een deelverzameling van Q' op Q, zodat
$\forall_{x \in X} [\lambda \tau_x \subseteq \tau_x' \lambda]$
$q' \in Q \lambda^{-1} \Rightarrow q' \lambda \tau_x \neq \emptyset \Rightarrow q' \lambda \tau_x = q' \tau_x' \lambda \Rightarrow q' \tau_x' \in Q \lambda^{-1}$
dwz. $(Q \lambda^{-1}; \{\tau_x' \mid x \in X\})$ is een deeltoestandsautomaat van $\mathcal{A}'$ met $D_{Q \times X'} \tau_x' \lambda = \lambda \tau_x$
Kies nu voor η de identiteit en voor ζ de afbeelding λ van $Q \lambda^{-1}$ in Q'.
Volgens 5.2.10. is nu de helft bewezen.

Nu is $\mathcal{A}$ een homomorf beeld van een deeltoestandsautomaat $\mathcal{A}''$ van $\mathcal{A}'$.
Dan bestaat er een afbeelding ζ van Q'' op Q en een afbeelding η van X'' op X, zodat
$\forall_{x \in X''} [\tau_x'' \zeta = \zeta \tau_{x\eta}]$.
$\tau_x'' \subseteq \tau_x' \Rightarrow \tau_x'' \zeta \subseteq \tau_x' \zeta$ $\Big\} \forall_{x \in X''} [\tau_x' \zeta \supseteq \zeta \tau_{x\eta}]$

6.1.13. Als $\mathcal{A}' \geq \mathcal{A}$, dan $(S_A,) \mid (S_{A'},)$.

bewijs: Volgens 6.1.12. is $\mathcal{A}$ een homomorf beeld van een deeltoestandsautomaat $\mathcal{A}''$ van $\mathcal{A}'$.
Volgens 5.2.14. is $(S_A,)$ een homomorf beeld van $(S_{A''},)$.
Volgens 5.2.9. is $(S_{A''},)$ een homomorf beeld van een ondersemigroep van $(S_{A'},)$.
Dus $(S_A,)$ is een homomorf beeld van een ondersemigroep van $(S_{A'},)$.

6.2. Toelaatbare en responsieconsistente overdekkingen

6.2.1. A is een automaat.
Een overdekking C van Q heet toelaatbaar als
$\forall_{x\in X}\,\forall_{B\in C}\,\forall_{B'\in C}\ [\ B\tau_x \subseteq B'\ ]$

Een overdekking C van Q heet responsieconsistent als
$\forall_{w\in X^*}\,\forall_{B\in C}\ [\ q\in B \wedge q'\in B \Rightarrow q\sigma_w = q'\sigma_w\ ]$.

6.2.2. Ψ is een zwak homomorfisme van A op A'.
De overdekking $C = \{q'\Psi^{-1} \mid q'\in Q'\}$ is een toelaatbare en responsieconsistente overdekking van Q.

bewijs: We spreken af: $q'_i \in Q'$ dan $q'_i\Psi^{-1} = B_i$.
$\mathrm{pr}_1\Psi = Q \Rightarrow$ C is een overdekking.
$B_i\tau_x = q'_i\Psi^{-1}\tau_x \subseteq q'_i\tau_{x'}\Psi^{-1} = q'_j\Psi^{-1} = B_j$
dus C is toelaatbaar.

$B_i\sigma_x = q'_i\Psi^{-1}\sigma_x \subseteq q'_i\sigma_{x'}$ en $|q'_i\sigma_{x'}| = 1$
dus C is responsieconsistent.

6.2.3. C is een toelaatbare en responsieconsistente overdekking.
A/C is een automaat met de volgende eigenschappen:
- er bestaat een een-eenduidige correspondentie tussen de toestanden van A/C en de blokken van C.
- het ingangsalfabet en responsiealfabet is gelijk aan die van A.
- τ^c is zodanig dat
$\underline{B_i}\tau^c_x = \underline{B_j} \Rightarrow B_i\tau_x \subseteq B_j$ en $\underline{B_i}\sigma^c_x = B_i\sigma_x$.

We noemen A/C de C-factor van A. De C-factor is eenduidig slechts C een partitie is.

6.2.4. Als C een toelaatbare en responsieconsistente overdekking is, dan is A/C een zwak homomorf beeld van A.

bewijs: We definiëren de relatie Ψ: $(q,B)\in\Psi \Leftrightarrow q\in B$.

$\forall_{B_i\in C}\,\forall_{x\in X}\ [\ B_i\Psi^{-1}\tau_x = B_{i'}\tau_x \subseteq B_j = B_j\Psi^{-1} = \underline{B_j}\tau^c_x\Psi^{-1}\ ]$.
$\forall_{B_i\in C}\,\forall_{x\in X}\ [\ B_i\Psi^{-1}\sigma_x = B_i\sigma_x = \underline{B_i}\sigma^c_x\ ]$.

6.3. Lusvrije combinaties van toestandsautomaten

6.3.1. $\mathcal{A}$ heet het direkt produkt van $\mathcal{A}_1$ en $\mathcal{A}_2$ als
$Q = Q_1 \times Q_2$;
$X = X_1 = X_2$;
$\forall_{x\in X}\ [\ ((q_1,q_2),(q'_1,q'_2)) \in \tau_x \Leftrightarrow (q_1,q'_1)\in\tau^1_x \wedge (q_2,q'_2)\in\tau^2_x\ ]$.
Notatie: $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$.

6.3.2. Vorming van direkte produkten van toestandsautomaten is associatief.

bewijs: Voor $(\mathcal{A}_1\otimes\mathcal{A}_2)\otimes\mathcal{A}_3$:
$Q = (Q_1\times Q_2)\times Q_3 = Q_1\times Q_2\times Q_3$;
$X = X_1 = X_2 = X_3$;
$((q_1,q_2),q_3)\,\tau_x = (q_1\tau^1_x, q_2\tau^2_x, q_3\tau^3_x)$.

Voor $\mathcal{A}_1\otimes(\mathcal{A}_2\otimes\mathcal{A}_3)$:
$Q = Q_1\times(Q_2\times Q_3) = Q_1\times Q_2\times Q_3$;
$X = X_1 = X_2 = X_3$;
$(q_1,(q_2,q_3))\,\tau_x = (q_1\tau^1_x, q_2\tau^2_x, q_3\tau^3_x)$.

6.3.3. μ_1 en μ_2 zijn twee toelaatbare partities van Q, waarvoor geldt:
$\forall_{B^1\in\mu_1}\ \forall_{B^2\in\mu_2}\ [|B^1\cap B^2|\leq 1]$

Dan $\mathcal{K}/\mu_1 \otimes \mathcal{K}/\mu_2 \geq \mathcal{K}$.

bewijs: $\mathcal{K}_1=\mathcal{K}/\mu_1$; $\mathcal{K}_2=\mathcal{K}/\mu_2$; $A_0=A/\mu_1\otimes A/\mu_2$.

De verzameling $Q'\subseteq Q\times Q$ is de verzameling
$\{(\underline{B}^1_i,\underline{B}^2_j)\mid B^1_i\cap B^2_j\neq\emptyset\}$
De afbeelding λ van Q' in Q wordt gedefinieerd door
$(\underline{B}^1_i,\underline{B}^2_j)\lambda = q\in B^1_i\cap B^2_j$.
Merk op dat λ een-eenduidig en surjectief is.
π_1 en π_2 zijn op te vatten als natuurlijke afbeeldingen van Q op de blokken van resp. μ_1 en μ_2, dwz.
$q\pi_1=B^1_i \Leftrightarrow q\in B^1_i$ en $q\pi_2=B^2_j\Leftrightarrow q\in B^2_j$.

$$\forall_{(B^1_i,B^2_j)\in Q'}\Big[(\underline{B}^1_i,\underline{B}^2_j)\lambda\tau_x = (B^1_i\cap B^2_j)\tau_x = B^1_i\tau_x\cap B^2_j\tau_x = B^1_i\tau_x\pi_1\cap B^2_j\tau_x\pi_2 = (\underline{B^1_i\tau_x\pi_1}\ ,\underline{B^2_j\tau_x\pi_2}) = (\underline{B}^1_i\tau'_x\ ,B^2_j\tau'_x)\lambda = (\underline{B}^1_i,\underline{B}^2_j)\tau'_x\circ\lambda\Big]$$

dwz, $\mathcal{K}_0\geq\mathcal{K}$.

6.3.4. A ,A_1 en A_2 zijn automaten.
ω is een afbeelding van $Q_1\times X_1$ in X_2.
$\mathcal{K}$ noemen we het ω-cascadeprodukt van $\mathcal{K}_1$ en $\mathcal{K}_2$ als
$Q=Q_1\times Q_2$
$\forall_{x\in X}\ [((q_1,q_2),(q'_1,q'_2))\in\tau_x \iff ((q_1,q'_1)\in\tau^1_x \wedge (q_2,q'_2)\in\tau^2_{(q_1,x)\omega})]$
Notatie: $\mathcal{K}=\mathcal{K}_1\textcircled{\omega}\mathcal{K}_2$.

Als $Q_1\times X_1\subseteq X_2$ en $\omega=D_{Q_1\times X_1}$, dan noteren we dit als $\mathcal{K}=\mathcal{K}_1\ominus\mathcal{K}_2$.

opm. Het is eenvoudig na te gaan dat de definitie correct is, dwz. A is volledig en deterministisch.

6.3.5. $\mathcal{K}_1\textcircled{\otimes}\mathcal{K}_2$ is op te vatten als een ω-cascadeprodukt van $\mathcal{K}_1$ en $\mathcal{K}_2$ met
$X_1=X_2$
$\forall_{q_1\in Q_1}\ [\omega(q_1,x)=x]$

6.3.6. Men kan de vorming van cascadeprodukten als associatief opvatten, mits men beperkingen aan de bijbehorende afbeeldingen mag opleggen.

bewijs: $\mathcal{K}'=(\mathcal{K}_1\textcircled{\alpha}\mathcal{K}_2)\textcircled{\beta}\mathcal{K}_3$ en $\mathcal{K}''=\mathcal{K}_1\textcircled{\gamma}(\mathcal{K}_2\textcircled{\delta}\mathcal{K}_3)$.
De index 1,2 hoort bij het toestandsautomaat $\mathcal{K}_1\textcircled{\alpha}\mathcal{K}_2$, terwijl 2,3 bij $\mathcal{K}_2\textcircled{\delta}\mathcal{K}_3$ hoort.

$Q'=(Q_1\times Q_2)\times Q_3=Q_1\times Q_2\times Q_3=Q_1\times(Q_2\times Q_3)=Q''$.
$X'=X'_{12}=X_1=X''$.

$$\forall_{q_1\in Q_1}\ \forall_{q_2\in Q_2}\ \forall_{q_3\in Q_3}\ \forall_{x\in X_1}\Big[(q_1,q_2,q_3)\tau'_x=((q_1,q_2)\tau'^{12}_x,q_3\tau^3_{((q_1,q_2),x)\beta}) = (q_1\tau^1_x,q_2\tau^2_{(q_1,x)\alpha},q_3\tau^3_{((q_1,q_2),x)\beta})\Big]$$
$$\forall_{q_1\in Q_1}\ \forall_{q_2\in Q_2}\ \forall_{q_3\in Q_3}\ \forall_{x\in X_1}\Big[(q_1,q_2,q_3)\tau''_x=(q_1\tau^1_x,(q_2,q_3)\tau^{23}_{(q_1,x)\gamma})= (q_1\tau^1_x,q_2\tau^2_{(q_1,x)\gamma},q_3\tau^3_{(q_2,(q_1,x)\gamma)\delta})\Big]$$

Als dus als volgt kiezen:
$\alpha=\gamma$ en
$\forall_{q_1\in Q_1}\ \forall_{q_2\in Q_2}\ \forall_{x\in X}[\beta((q_1,q_2),x)=\delta(q_1,\gamma(q_1,x))$
dan geldt:
$(\mathcal{K}_1\textcircled{\alpha}\mathcal{K}_2)\textcircled{\beta}\mathcal{K}_3=\mathcal{K}_1\textcircled{\gamma}(\mathcal{K}_2\textcircled{\delta}\mathcal{K}_3)$.

6.3.7. Als
$Q_1 \times X_1 \subseteq X_2$, $Q_1 \times Q_2 \times X_1 \subseteq X_3$, $Q_2 \times X_2 \subseteq X_3$ en
$\tau^3_{(q_0,q_1),x} = \tau^3_{(q_1,(q_0,x))}$,
dan $(K_1 \ominus K_2) \ominus K_3 = K_1 \ominus (K_2 \ominus K_3)$

bewijs: 6.3.6.

6.3.8. Als $K_1 \geq K_2$, dan bestaat er voor elke $K_0 \textcircled{\omega} K_2$ een afbeelding ω_1, zodat $K_0 \textcircled{\omega_1} K_1 \geq K_0 \textcircled{\omega_2} K_2$.

bewijs: De index 0,1 hoort bij $K_0 \textcircled{\omega} K_1$ en 0,2 bij $K_0 \textcircled{\omega} K_2$.
We bewijzen de stelling in de zin van 6.1.3.!

Er bestaat een afbeelding λ uit Q_1 op Q_2 en een afbeelding ξ van X_2 in X_1, waarvoor
$\forall_{x \in X_2} [\lambda \tau^2_x \subseteq \tau^1_{x\xi} \lambda]$
We definiëren de afbeelding λ' van $Q_0 \times Q_2 \lambda^{-1}$ op $Q_0 \times Q_2$ als
$(q_0, q_1)\lambda' = (q_0, q_1 \lambda)$.
Verder laten we voor ω_1 gelden
$\forall_{q_0 \in Q_0} \forall_{x \in X_0} [(q_0, x)\omega_1 = (q_0, x)\omega_2 \xi]$

$$\forall_{(q_0,q_1) \in Q_0 \times Q_2 \lambda^{-1} \subseteq Q_{0,1}} \forall_{x \in X_0} \Big[(q_0,q_1)\lambda' \tau^{0,2}_x = (q_0,q_1\lambda)\tau^{0,2}_x = (q_0 \tau^0_x, q_1 \lambda \tau^2_{(q_0,x)\omega_2}) = (q_0 \tau^0_x, q_1 \tau^1_{(q_0,x)\omega_2 \xi} \lambda) = (q_0,q_1)\tau^{0,1} \Big].$$

Dwz. $K_0 \textcircled{\omega_1} K_1 \geq K_0 \textcircled{\omega_2} K_2$.

6.3.9. Als $K_1 \geq K_2$ met $\xi = D_X$, dan $K_0 \ominus K_1 \geq K_0 \ominus K_2$.

bewijs: 6.3.8.

6.3.10. Als $K_1 \geq K_2$ met ξ als een een-eenduidige afbeelding, bestaat er voor elke $K_2 \textcircled{\omega} K_0$ een afbeelding ω_1, zodat $K_1 \textcircled{\omega} K_0 \geq K_2 \textcircled{\omega} K_0$.

bewijs: De index 1,0 hoort bij $K_1 \textcircled{\omega} K_0$ en 2,0 bij $K_2 \textcircled{\omega} K_0$.

Er bestaat een afbeelding λ uit Q_1 op Q_2 en een afbeelding ξ van X_2 in X_1, waarvoor
$\forall_{x \in X_2} [\lambda \tau^2_x \subseteq \tau^1_{x\xi} \lambda]$
We definiëren de afbeelding λ' van $Q_2 \lambda^{-1} \times Q_0$ op $Q_2 \times Q_0$ als
$(q_1, q_0)\lambda' = (q_1 \lambda, q_0)$.
Verder laten we voor ω_1 gelden
als $q_1 \in Q_2 \lambda^{-1}$ en $x \in X_2$, dan $(q_1, x\xi)\omega_1 = (q_1 \lambda, x)\omega_2$ en anders willekeurig.

$$\forall_{(q_1,q_0) \in Q_2 \lambda^{-1} \times Q_0 \subseteq Q_{1,0}} \forall_{x \in X_2} \Big[(q_1,q_0)\lambda' \tau^{1,0}_x = (q_1\lambda, q_0)\tau^{3,0}_x = (q_1 \lambda \tau^2_x, q_0 \tau^0_{(q_1,\lambda,x)\omega_2}) = (q_1 \tau^1_{x\xi} \lambda, q_0 \tau^0_{(q_1,x\xi)\omega_1}) = (q_1 \tau^1_{x\xi}, q_0 \tau^0_{(q_1,x\xi)\omega_1})\lambda' = (q_1,q_0)\tau^{1,0}_{x\xi}\lambda' \Big]$$

Dwz. $K_1 \textcircled{\omega_1} K_0 \geq K_2 \textcircled{\omega_2} K_2$.

opm. De voorwaarde dat ξ een-eenduidig moet zijn, is bij de definiëring van ω_1 gebruikt. We kunnen K_1 echter zo modificeren, dat we deze voorwaarde kunnen laten vallen:
Stel ξ is niet een-eenduidig, dan zijn er $x_1, x_2, \ldots, x_p \in X_2$ waarvoor $x_1\xi = x_2\xi = \ldots = x_p\xi$. Uit 6.1.3. weten we dan dat $\tau^2_{x_1} = \tau^2_{x_2} = \ldots = \tau^2_{x_p}$.
We voegen nu aan X_1 p-1 ingangssymbolen toe. De hierbij behorende afbeeldingen τ^k_x maken we alle gelijk aan $\tau^1_{x_1\xi}$. Zo behandelen we ieder deelverzameling van X_2, bestaande uit elementen met hetzelfde beeld onder ξ.
Zo ontstaat een nieuw toestandsautomaat K'_1, waarvoor geldt:
$\left.\begin{matrix} K'_1 \geq K_1 \\ K_1 \geq K_2 \end{matrix}\right\} \Rightarrow K'_1 \geq K_2$ met ξ als een een-eenduidige afbeelding.
We kunnen hierop de stelling 6.3.10. op toepassen.
We constateren verder dat $(S_{A_1}, \ ) = (S_{A'_1}, \ )$.

6.3.11. Als μ een toelaatbare partitie van Q is, dan bestaat er een toestandsautomaat A_1, zodat
$|Q_1| = \#\mu$ en
$A/\mu \ominus A_1 \geq A$.

bewijs: Men kan een partitie μ_1 van Q vinden, zodat
$\forall_{B\in\mu}\ \forall_{B'\in\mu,}\ [|B \cap B'| \leq 1]$ en $= \#$.
Bv. door de elementen van elk blok $B \in \mu$ te nummeren van 1 t/m $|B|$; voor μ_1 kan men dan de blokken van elementen met gelijke nummers nemen.

$Q_1 = \mu_1$ en $X_1 = \mu \times X$
$\underline{B}'_j\, \tau'_{(Q_i,x)} = (B'_j \cap B_i)\tau_x \pi_1$, waarbij π_1 de natuurlijke afbeelding van Q op μ_1 is: $q\ \pi_1 = B'_i \Leftrightarrow q \in B'_i$.
$Q'' \subseteq \mu \times Q_1 = \mu \times \mu_1$ is de verzameling van die $(\underline{B}_i, \underline{B}'_j)$ waarvoor $B_i \cap B'_j \neq \emptyset$.

λ is een 1-1-afbeelding van Q" op Q met $(\underline{B}_i, \underline{B}'_j)\lambda = q \in B_i \cap B'_j$.
π is de natuurlijke afbeelding van Q op μ en $A_0 = A/\mu$.

$\forall_{(Q_i,Q'_j)\in Q''}\ [(\underline{B}_i, \underline{B}'_j)\lambda\tau_x = (B_i \cap B'_j)\tau_x = B_i\tau_x\pi \cap (B_i \cap B'_j)\tau_x\pi_1 =$
$= (B_i\tau_x\pi\ ,(B_i \cap B'_j)\tau_x\pi_1)\lambda = (\underline{B}_i\,\tau_x^o, \underline{B}'_j\,\tau'_{(Q_i,x)})\lambda = (\underline{B}_i, \underline{B}'_j)\tau_x^{o'}\lambda$.
Dwz. $A/\mu \ominus A_1 \geq A$.

6.3.12. Als C een toelaatbare overdekking van Q is, dan bestaan er toestandsautomaten A_1 en A_2, waarvoor geldt, dat A_1 isomorf is met de C-factor van A en $|Q_2| = \#C$, terwijl verder $A_1 \ominus A_2 \geq A$.

bewijs: We construeren een toestandsautomaat A' op de volgende manier:
$X' = X$
$Q' = \{(q, \underline{B}_i) \mid q \in Q \wedge B_i \in C \wedge q \in B_i\}$.
$(q, \underline{B}_i)\tau'_x = (q\,\tau_x, \underline{B}_i\tau_x^c)$.
Het rechterlid is een element van Q', want $q \in B_j \Rightarrow q\tau_x \in B_j$ met $\underline{B}_j = \underline{B}\,\tau_x^c$

Voor μ_1 nemen we die partitie van Q' die de elementen met gelijke tweede component in een blok samenbrengt. Dan is μ_1 toelaatbaar en $A'/\mu_1 \simeq A/C$, zoals gemakkelijk kan worden nagegaan.

Neem nu de afbeelding λ van Q' op Q met $(q, \underline{B}_i)\lambda = q$; dan is voldaan aan $\lambda\tau_x = \tau'_x\lambda$, omdat $(q, \underline{B}_i)\lambda\tau_x = q\tau_x$ en $(q, \underline{B}_i)\tau'_x\lambda = (q\tau_x, \underline{B}_i\tau_x^c)\lambda = q\tau_x$.
Dit betekent, dat $A' \geq A$.

Volgens 6.3.11. bestaat er nu een A_2, zodat $A_1 \ominus A_2 \geq A'$, waarin $A_1 = A'/\mu_1$ en $|Q_2| = \#\mu_1$.
Daar verder $A' \geq A$, $A'/\mu_1 \simeq A/C$ en $\#C = \#\mu_1$ is het bewijs geleverd.

7. Ontleedbaarheid

7.1. Permutaties en resets

7.1.1. $\mathcal{A}$ heet een permutatie-reset-toestandsautomaat als
$\forall_{x\in X}\ [\,|Q\tau_x|=1 \vee |Q\tau_x|=|Q|\,]$.

$\mathcal{A}$ heet een permutatie-toestandsautomaat als
$\forall_{x\in X}\ [\,|Q\tau_x|=|Q|\,]$.

$\mathcal{A}$ heet een reset-toestandsautomaat als
$\forall_{x\in X}\ [\,|Q\tau_x|=1 \vee \forall_{q\in Q}[q\tau_x=q]\,]$.

7.1.2. Als $|Q|\geq 2$, dan kan $\mathcal{A}$ gerealiseerd worden als een cascadeprodukt van $|Q|-1$ permutatie-reset-toestandsautomaten.

bewijs: μ is het verzamelingensysteem van Q, dat alle deelverzamelingen van Q bevat, die $|Q|-1$ elementen bevatten. μ is altijd toelaatbaar.

We construeren nu een μ-factor van $\mathcal{A}$, aangegeven met $\mathcal{A}'$, die voldoet aan:
$\forall_{B_1\in Q'}\ \forall_{B_1'\in Q'}\ \forall_{B_2\in Q'}\ \forall_{B_2'\in Q'}\ \forall_{x\in X}\,[|Q\tau_x|<|Q| \wedge \underline{B}_1\tau_x=\underline{B}_1' \wedge \underline{B}_2\tau_x=\underline{B}_2' \Rightarrow \underline{B}_1'=\underline{B}_2']$.

Dan geldt nl. dat als $|Q\tau_x|<|Q|$, $|Q'\tau_x'|=1$. En verder als $|Q\tau_x|=|Q|$, dan is τ_x een permutatie en dan is er voor elk blok B van μ slechts één blok B' van μ waarvoor $B\tau_x\subseteq B'$, en $B_1\neq B_2 \Rightarrow \underline{B}_1\tau_x' \neq \underline{B}_2\tau_x'$. Dwz. dat ook τ_x' een permutatie is.
Dit betekent dat $\mathcal{A}'$ een permutatie-reset-toestandsautomaat is.
Volgens 6.3.12. kunnen we $\mathcal{A}$ realiseren met een cascadeprodukt $\mathcal{A}_1\ominus\mathcal{A}_2$, waarin $\mathcal{A}_1$ een permutatie-reset-toestandsautomaat is en $|Q_1|=\#\mu=|Q|-1$.

Met $\mathcal{A}_2$ kunnen we hetzelfde doen en we verkrijgen, dan $\mathcal{A}_2'\ominus\mathcal{A}_3$, waarvoor geldt:
$\mathcal{A}_2'\ominus\mathcal{A}_3 \geq \mathcal{A}_2$, $|Q_3|=|Q|-2$ en $\mathcal{A}_2'$ is een permutatie-reset-toestandsautomaat.

Volgens 6.3.9. : $\mathcal{A}_1\ominus(\mathcal{A}_2'\ominus\mathcal{A}_3)\geq\mathcal{A}_1\ominus\mathcal{A}_2\geq\mathcal{A}$.

Zo kan men verder gaan tot $\mathcal{A}_{|Q|-1}$, waarvoor $|Q_{|Q|-1}|=|Q|-(|Q|-2)=2$.
Daar elk toestands automaat met 2 toestanden een permutatie-reset-toestandsautomaat is, is het bewijs hiermee volledig.

7.1.3. Elk permutatie-reset-toestandsautomaat kan gerealiseerd worden met een cascadeprodukt van een permutatie- en een reset-toestandsautomaat.

bewijs: Zij $\mathcal{A}$ een permutatie-reset-toestandsautomaat.
$X_r:=\{x\,|\,x\in X \wedge |Q\tau_x|=1\}$ en $X_p:=\{x\,|\,x\in X \wedge |Q\tau_x|=|Q|\}$.
$(\langle\{\tau_x\,|\,x\in X_p\}\rangle,\ )$ is een ondergroep van $(S_A,\ )$, die we met $(G_p,\ )$ aangeven.
We definiëren een volledig, deterministisch toestandsautomaat $\mathcal{A}_1$ met
$Q_1=G_p$, $X_1=X$ en
$\forall_{\tau_\omega\in G_p}\ \forall_{x\in X}\,[(x\in X_r \Rightarrow (\tau_\omega)\tau_x'=\tau_\omega) \wedge (x\in X_p \Rightarrow (\tau_\omega)\tau_x'=\tau_{\omega x})]$.
en een volledig, deterministisch toestandsautomaat $\mathcal{A}_2$ met $Q_2=Q$, $X_2=G_p\times X$ en
$\forall_{q\in Q_2}\ \forall_{(\tau_\omega,x)\in X_2}\,[(x\in X_r \Rightarrow q\,\tau^2_{(\tau_\omega,x)}=q\,\tau_x\tau_\omega^{-1}) \wedge (x\in X_p \Rightarrow q\,\tau^2_{(\tau_\omega,x)}=q)]$.
Zij $\mathcal{A}'=\mathcal{A}_1\ominus\mathcal{A}_2$. $\mathcal{A}_1$ is een permutatie-, $\mathcal{A}_2$ een reset-toestandsautomaat!
λ is een afbeelding van $Q_1\times Q_2$ op Q met $(\tau_\omega,q_2)\lambda=q \Leftrightarrow q_2\tau_\omega=q$.

$\forall_{(\tau_\omega,q_2)\in Q_1\times Q_2}\ \forall_{x\in X_r}[(\tau_\omega,q_2)\lambda\tau_x=q_2\tau_\omega\tau_x=q_2\tau_x=q_2\tau_x\tau_{\omega x}^{-1}\tau_{\omega x}=(\tau_\omega,q_2\tau_x\tau_{\omega x}^{-1})\lambda=(\tau_\omega,q_2)\tau_x'\lambda]$
$\forall_{(\tau_\omega,q_2)\in Q_1\times Q_2}\ \forall_{x\in X_p}[(\tau_\omega,q_2)\lambda\tau_x=q_2\tau_\omega\tau_x=q_2\tau_{\omega x}=(\tau_{\omega x},q_2)\lambda=(\tau_\omega,q_2)\tau_x'\lambda]$
Dus $\mathcal{A}'=\mathcal{A}_1\ominus\mathcal{A}_2\geq\mathcal{A}$.

7.1.4. Elke reset-toestandsautomaat kan met een direkt produkt van reset-toestandsautomaten met elk twee toestanden gerealiseerd worden.

bewijs: Zij $\mathcal{A}$ een reset-toestandsautomaat. Hiervoor is elke partitie toelaatbaar en de bijbehorende factor is weer een reset-toestandsautomaat.
Neem daarom een partitie μ met $|\mu|=2$, dan geldt $\#\mu<|Q|$, en dus kan, volgens 6.3.3., $\mathcal{A}$ gerealiseerd worden met $\mathcal{A}/\mu \otimes \mathcal{A}'$, waarbij $|Q'|<|Q|$.
Als $|Q'|>2$ kan men op $\mathcal{A}'$ dezelfde procedure toepassen.
Daar verder geldt (direkt produkt is een speciaal geval van cascade!)
$((\mathcal{A}/\mu \otimes \mathcal{A}') \geq \mathcal{A}) \wedge (\mathcal{A}'_1 \otimes \mathcal{A}'_2 \geq \mathcal{A}')) \Rightarrow \mathcal{A}/\mu \otimes (\mathcal{A}'_1 \otimes \mathcal{A}'_2) \geq \mathcal{A}$.
Q is eindig, dus eens zalde laatste automaat ook twee toestanden hebben.

opm. Het aantal automaten dat nodig is, is gelijk aan het eerste gehele getal boven $^2\log|Q|$.

7.2. Groep-toestandsautomaten

7.2.1. $(G, \circ)$ is een groep.
Een toestandsautomaat $\mathcal{A}$ waarvoor geldt
$Q=G$, $X=G$, en
$\forall_{g_1\in Q}\ \forall_{g_2\in X}\ [g_1\tau_{g_2}=g_1 g_2]$
heet een groep-toestandsautomaat.
We geven haar aan met $\mathcal{G}$.

7.2.2. Als $\mathcal{A}$ een permutatie-toestandsautomaat is, dan $\mathcal{G}_{\mathcal{A}} \geq \mathcal{A}$.

bewijs: λ is de afbeelding uit $S_{\mathcal{A}}$ op Q en wel zo, dat $\tau_\omega\lambda = q_0\tau_\omega$, waarbij q_0 willekeurig gekozen kan worden.
ξ is de 1-1-afbeelding van X in $S_{\mathcal{A}}$, waarvoor $x\xi=\tau_x$.
Dan geldt:
$\forall_{x\in X}\ [\tau_\omega\lambda\tau_x = q_0\tau_\omega\tau_x = q_0\tau_\omega\tau'_{\tau_x} = q_0\tau_\omega\tau'_{x\xi} = \tau_\omega\tau'_{x\xi}\lambda]$

7.2.3. $(G, \circ)$ is een groep en $(H, \circ) \lhd (G, \circ)$.
$(G/H, \circ)$ geven we aan met F.
Er bestaan twee toestandsautomaten $\mathcal{A}_1$ en $\mathcal{A}_2$ waarvoor
$\mathcal{A}_1 \otimes \mathcal{A}_2 \geq \mathcal{G}$, $\mathcal{A}_1 \simeq \mathcal{F}$ en $\mathcal{A}_2 \cong \mathcal{H}$.

bewijs: We kiezen in elke nevenklasse van H een element, dat we de representant noemen. Als $g\in G$ een element van de nevenklasse met representant c is, dan noteren we dat als $\overline{g}=c$.
$Q_1=\{\overline{g}\mid g\in G\}$ en $X_1=G$.
$\forall_{c\in Q_1}\ \forall_{g\in X_1}\ [c\tau'_g=\overline{(cg)}]$
De afbeelding ζ die elke nevenklasse op haar representant afbeeldt is een-eenduidig en $\eta=D_G$.
$\forall_{g\in G}[[\overline{g}]\tau'^{H}_{g}\zeta = [g\overline{g'}]\zeta = \overline{(g\overline{g'})} = [g]\zeta\tau'_g$, dwz. $\mathcal{A}\simeq\mathcal{F}$.

$Q_2=\{g\mid g\in H\}$ en $X_2=\{g\mid g\in H\}$.
$\forall_{h_1\in H}\ \forall_{h_2\in H}[h_1\tau^2_{h_2}=h_1h_2]$, dwz. $\mathcal{A}_2=\mathcal{H}$.

De afbeelding van $Q_1\times G$ in X_2: $(c,g)\omega = cg\overline{(cg)}^{-1}$. $(c,g)\omega\in H$, immers
$cg\in H(cg) \Rightarrow \exists_{h\in H}[cg=h(cg)] \Rightarrow cg(cg)^{-1}=h\in H$.
Voor de afbeelding λ geldt: $\forall_{c\in Q}\ \forall_{h\in H}[(c,h)\lambda = hc]$
$\forall_{c\in Q_1}\ \forall_{h\in Q_2}\ \forall_{g\in G}\ [(c,h)\lambda\tau_g = hc\tau_g = hcg = (\overline{(cg)}, hcg\overline{(cg)}^{-1})\lambda = (c\tau'_g, h\tau'^{-1}_{cg\overline{(cg)}^{-1}})\lambda =$
$= (c\tau'_g, h\tau^2_{(c,g)\omega})\lambda = (c,h)\tau^{12}_g\lambda]$
Dus $\mathcal{A}_1\otimes\mathcal{A}_2 \geq \mathcal{G}$.

7.2.4. Elke groep-toestandsautomaat $\mathcal{A}$ kan gerealiseerd worden als een cascadeprodukt van groep-toestandsautomaten, waarvan de groepen de factoren zijn van de compositierij van G. Deze groepen zijn dus enkelvoudig.

bewijs: Voor elke eindige groep G bestaat er een (op volgorde na eenduidig bepaalde (4.2.49.)) compositierij (4.2.47.):
$(G,)=(G_0,) \triangleright (G_1,) \triangleright \ldots\ldots \triangleright (G_k,)=(\{e\},)$.
We geven $(G_{i-1}/G_i,)$ aan met $(F_i,)$.

Volgens 7.2.3. kan $\mathcal{A}$ gerealiseerd worden door een cascade $\mathcal{A}_1 \textcircled{\omega_1} \mathcal{A}_2$ met $\mathcal{A}_1$ isomorf met $\mathcal{A}_1$ en $\mathcal{A}_2=\mathcal{A}_1$.
Volgens 7.2.3, kan ook $\mathcal{A}_1$ gerealiseerd worden door een cascade $\mathcal{A}_2' \textcircled{\omega_2} \mathcal{A}_3$ met $\mathcal{A}_1' \simeq \mathcal{A}$ en $\mathcal{A}_3=\mathcal{A}$.
Volgens 6.3.8. bestaat er nu een ω_1', zodat
$\mathcal{A}_1 \textcircled{\omega_1'} (\mathcal{A}_2' \textcircled{\omega_2} \mathcal{A}_3) \geq \mathcal{A}$.
Op deze manier kunnen we verder gaan tot $(G_{k-1}/G_k,) \simeq (G_{k-1},)$.
Daar de factoren van een compositierij alle enkelvoudig zijn, zijn de groepen van de groep-toestandsautomaten in de cascade alle enkelvoudig.

7.2.5. Elke toestandsautomaat kan gerealiseerd worden door een cascadeprodukt van toestandsautomaten, terwijl voor zo'n toestandsautomaat, dat in de cascade voorkomt, geldt:
óf hij is een groep-toestandsautomaat waarvan de groep enkelvoudig is,
óf hij is een reset-toestandsautomaat met twee toestanden.

bewijs: 7.1.2.: Elke toestandsautomaat is te ontleden in een cascade van permutatie-reset-toestandsautomaten.
7.1.3.: Elke permutatie-reset-toestandsautomaat is te ontleden in een cascade van een groep- en een reset-toestandsautomaat.
(1): Dus elke toestandsautomaat kan ontleed worden tot een cascade van groep- en reset-toestandsautomaten.
7.2.4.: Elke groep-toestandsautomaat is te ontleden in groep-toestandsautomaten waarvan de groep enkelvoudig is.(in cascade)
7.1.4.: Elke reset-toestandsautomaat kan gerealiseerd worden als een direkt produkt van reset-toestandsautomaten met twee toestanden.
6.3.5.: Een direkt produkt is op te vatten als een speciale cascadevorm.

(1), 7.2.4., 7.1.4., 6.3.5., 6.3.8. en 6.3.10. leveren nu de stelling.

7.3. Hoofdstelling

7.3.1. De maat van $\mathcal{A}$ is een geordend tripel van getallen, gedefinieerd door:
$m(A)=(|<\{\tau_\omega | (\tau_\omega \in S_A) \wedge (|Q\tau_\omega| \neq 1)\}>|, |Q|, |S_A|)$.

Als $m(A)=(a,b,c)$ en $m(A')=(a',b',c',)$, dan
$m(A) > m(A') \Leftrightarrow (a>a') \vee (a=a' \wedge b>b') \vee (a=a' \wedge b=b' \wedge c>c')$

7.3.2. Voor elke toestandsautomaat $\mathcal{A}$ is $*\mathcal{A}$ het deeltoestandsautomaat van $\mathcal{A}$ met
$*Q=Q$, $*X=X \setminus \{x \mid |Q\tau_x|=1\}$ en $\forall_{x \in *X} [*\tau_x = \tau_x]$.

7.3.3. (S,) is een monoïde van afbeeldingen van Q in Q, waarbij Q een eindige verzameling is.

$S* = <\{\sigma \mid \sigma \in S \wedge |Q\sigma| \neq 1\}>$.

We spreken verder af: $S* = \{\Lambda\}$ als $|Q|=1$

7.3.4. Als $\mathcal{A}$ noch een permutatie- noch een reset-toestandsautomaat met twee toestanden is, dan geldt één van de volgende drie beweringen:
1. $*\mathcal{A}$ heeft een deeltoestandsautomaat $\mathcal{A}'$ waarvoor geldt: $X'=*X$ en $|*Q| > |Q'| > 1$.
2. S_A bevat een permutatie ongelijk aan de identiteit.
3. $S_A = V \cup T$, waarin $(V,)$ een ondersemigroep van S_A is met $|V*| < |S_A*|$ en T een echt linkerideaal van $(S_A \setminus \{\Lambda\},)$ is.

bewijs: We bewijzen deze stelling door uit de ontkenning van de beweringen 1 en 2 de bewering 3 af te leiden.

$S := S_A \setminus \{\Lambda\}$. $(S,)$ is een ondersemigroep van $(S_A,)$, want S_A bevat geen permutaties ongelijk aan de identiteit.
$\exists_{\sigma \in S} [|Q\sigma| > 1]$, want anders zou $\mathcal{A}$ een reset-toestandsautomaat zijn en is bewering 1 van toepassing.
Als $S_A\sigma \cup \{\rho \mid |Q\rho| = 1 \wedge \rho \in S\} = S$, dan zou $*\mathcal{A}$ een deeltoestandsautomaat hebben als in 1 met $Q' = Q\sigma$. Dus $S_A\sigma \cup \{\rho \mid |Q\rho| = 1 \wedge \rho \in S\} \subset S$.
Dan is $S_A\sigma$ een echt linkerideaal van $(S,)$ en dan bestaat er ook een maximaal linkerideaal T : (dwz. $(T \neq S) \wedge (T \subseteq I \subseteq S) \wedge (SI \subseteq I) \Rightarrow (I = S) \vee (I = T)$)
$V := S_A\nu \cup \{\Lambda\}$ voor een willekeurige $\nu \in S \setminus T$.
We constateren nu dat $(V \setminus \{\Lambda\}) \cup T$ een linkerideaal van $(S,)$ is, dat T bevat en niet gelijk is aan T, dwz. $(V \setminus \{\Lambda\}) \cup T = S$ en dus $V \cup T = S$.
Als $|Q\nu| > 1$, dan weten we reeds dat $V \cup \{\rho \mid \rho \in S \wedge |Q\rho| = 1\} \subset S_A$, waaruit volgt $|V*| < |S_A*|$.
In het andere geval, $|Q\nu| = 1$, geldt voor alle $\sigma \in S_A\nu$: $|Q\sigma| = 1$ en dan geldt $|V*| = 1 < |S_A*|$.

7.3.5. Als $\mathcal{A}$ noch een permutatie- noch een reset-toestandsautomaat is, dan bestaan er toestandsautomaten $\mathcal{A}_1$ en $\mathcal{A}_2$, zodat
$\mathcal{A}_1 \circledcirc \mathcal{A}_2 \geq \mathcal{A}$;
$(S_{A_1}*,) \mid (S_A,)$ en óf $m(A_1) < m(A)$, óf $\mathcal{A}_1$ is een permutatie-toestandsautomaat, óf $\mathcal{A}_1$ is een reset-toestandsautomaat met twee toestanden;
$(S_{A_2}*,) \mid (S_A,)$ en $m(A_2) < m(A)$.

bewijs: We bewijzen de stelling achtereenvolgens voor de gevallen 1,2,3 van 7.3.4..
1. $Q_2 = Q'$ en $Q_1 = Q \setminus Q_2 \cup \{\underline{q}\}$ waarbij $\underline{q} \notin Q$.

$$(q_1, q_2)\tau_x'' = \begin{cases} (q_1\tau_x, q_2) & \text{als } q_1 \neq \underline{q} \text{ en } q_1\tau_x \notin Q_2 \\ (\underline{q}, q_1\tau_x) & \text{als } q_1 \neq \underline{q} \text{ en } q_1\tau_x \in Q_2 \\ (q_0, q_1) & \text{als } Q\tau_x = \{q_0\} \text{ en } q_0 \in Q \setminus Q_2 \\ (q_1, q_2\tau_x) & \text{in alle andere gevallen.} \end{cases}$$

τ_x'' is hiermee volledig gedefinieerd, en ook correct, immers, als $|Q\tau_x| \geq 1$, dan $q\tau_x \in Q_2 = Q'$. Het vierde geval is dus alleen van toepassing als $q_1 = \underline{q}$ én $q_2\tau_x \in Q' = Q_2$.

Kiest men nu een afbeelding ς van $Q_1 \times Q_2$ in Q met $\begin{cases} (q_1, q_2)\varsigma = q_1 \text{ als } q_1 \neq \underline{q} \\ (q_1, q_2)\varsigma = q_2 \text{ als } q_1 = \underline{q} \end{cases}$

voor de vier gescheiden gevallen geldt dan:

$$(q_1, q_2)\tau_x''\varsigma = \left\{ \begin{array}{l} (q_1\tau_x, q_2)\varsigma = q_1\tau_x = \\ (\underline{q}, q_1\tau_x)\varsigma = q_1\tau_x = \\ (q_0, q_1)\varsigma = q_0 = q_1\tau_x = \\ (q_1, q_2\tau_x)\varsigma = q_2\tau_x = \end{array} \right\} (q_1, q_2)\varsigma\tau_x \quad . \Rightarrow \mathcal{A} \text{ is een homomorf beeld van } \mathcal{A}_1 \circledcirc \mathcal{A}_2 .$$

Volgens 6.1.12.: $\mathcal{A}_1 \circledcirc \mathcal{A}_2 \geq \mathcal{A}$.

$\mu = \{\{q\} \mid q \in Q \setminus Q'\} \cup \{Q'\}$ is een toelaatbare partitie van Q.
φ is nu een afbeelding van Q_1 op μ : $q\varphi = \{q\}$ als $q \neq \underline{q}$
$\underline{q}\varphi = Q'$.

Voor de vier gevallen geldt nu:

$$q\tau_x'\varphi = \left\{\begin{array}{l} q\tau_x\varphi = \{q\tau_x\} = \{q\}\tau_x'' = \\ \underline{q}\varphi = Q' \qquad\qquad = \\ q_0\varphi = \{q_0\} = \{q\}\tau_x'' \quad = \\ q\varphi = \underline{q}\varphi = Q' \quad = \end{array}\right\} q\varphi\tau_x''. \Rightarrow K/\mu \simeq K .$$

Volgens 5.2.12. en 5.2.14.: $(S_{A_1},)$ is een homomorf beeld van $(S_A,)$.
Hieruit volgt $(S_{A_1}*,) \mid (S_A,)$ en $|S_{A_1}| \leq |S_A|$: Ook $|S_{A_1}*| \leq |S_A*|$:
Bovendien $|Q_1| = |Q \setminus Q'| + 1 < |Q|$, omdat $|Q'| > 1$.
Dus $m(A_1) < m(A)$.
Uit de definitie van τ_x'' blijkt, dat $\tau''_{(q,x)}$ in het eerste en derde geval de identiteit is en in het tweede een constante afbeelding.
Dwz. $S_{A_2}* = \{D_Q, \sigma \mid \sigma \in S_A*\}$, waaruit volgt dat $(S_{A_2}*,)$ een homomorf beeld van een ondersemigroep van $(S_A,)$ is $\Rightarrow (S_{A_2}*,) \mid (S_A,)$.
Daar bovendien $|Q'| < |Q|$, geldt ook $m(A_2) < m(A)$

2. $P = <\{\sigma \mid \sigma \in S_A \wedge |Q\sigma| = |Q|\}>$.
$T = S_A \setminus P$.
K is geen permutatie-toestandsautomaat, dus $T \neq \emptyset$. T is een ideaal van $(S_A,)$.
$Q_1 = P$ en $Q_2 = Q$

$$(\sigma, q_2)\tau_x'' = \left\{\begin{array}{ll} (\sigma\tau_x, q_2) & \text{als } \tau_x \in P \\ (\sigma, q_2\sigma\tau_x\sigma^{-1}) & \text{als } \tau_x \in T \end{array}\right.$$

Ditmaal definiëren we de afbeelding φ van $Q_1 \times Q_2$ in Q met $(\sigma, q_2)\varphi = q_2\sigma$.

$$(\sigma, q_2)\tau_x''\varphi = \left\{\begin{array}{l} (\sigma\tau_x, q_2)\varphi = q_2\sigma\tau_x \quad = \\ (\sigma, q_2\sigma\tau_x\sigma^{-1})\varphi = q_2\sigma\tau_x = \end{array}\right\} (\sigma, q_2)\varphi\tau_x .$$

φ is dus een homomorfisme van $K_1 \textcircled{\omega} K_2$ op K, waaruit volgt $K_1 \textcircled{\omega} K_2 \geq K$.
$(S_{A_1},) = (P,) \Rightarrow (S_{A_1}*,) \mid (S_A,)$ en K_1 is een permutatie-toestands-automaat.
$(S_{A_2},) = (T,) \Rightarrow (S_{A_2}*,) \mid (S_A,)$.
Verder bevat $S_{A_2}*$ de niet-identiteitspermutaties van S_A* niet $\Rightarrow m(A_2) < m(A)$.

3. $Q_1 = V$ en $Q_2 = Q$.

$$(\sigma, q)\tau_x'' = \left\{\begin{array}{ll} (\sigma\tau_x, q) & \text{als } \tau_x \in V \setminus T \\ (\tau_\Lambda, q\sigma\tau_x) & \text{als } \tau_x \in T \end{array}\right.$$

φ definiëren we nu met $(\sigma, q)\varphi = q\sigma$.
Dan is φ een homomorfisme van $K_1 \textcircled{\omega} K_2$ op K, want

$$(\sigma, q)\tau_x''\varphi = \left\{\begin{array}{l} (\sigma\tau_x, q)\varphi = q\sigma\tau_x = \\ (\tau_\Lambda, q\sigma\tau_x)\varphi = q\sigma\tau_x = \end{array}\right\} (\sigma, q)\varphi\tau_x .$$

Dus $K_1 \textcircled{\omega} K_2 \geq K$.
$S_{A_1} = <V \setminus T> \Rightarrow (S_{A_1}*,)$ is een ondermonoïde van $(V,) \Rightarrow (S_{A_1}*,) \mid (V,) \Rightarrow$
$\Rightarrow (S_{A_1}*,) \mid (S ,)$.
$\forall_{\varphi \in V} [\, |Q\varphi| = 1 \Rightarrow |V\varphi| = 1] \Rightarrow (S_{A_1}*,)$ is isomorf met een ondermonoïde van $(V*,) \Rightarrow |S_{A_1}*| \leq |V*| \leq |S_A*| \Rightarrow m(A_1) < m(A)$.
$S_{A_2} = T \cup \{\Lambda\} \Rightarrow (S_{A_2},) \mid (S ,) \wedge (S_{A_2}*,) \mid (S_A,)$.
Tevens volgt hieruit: $|S_{A_2}*| \leq |S_A*|$
T is een echt ideaal: $|S_{A_2}| \leq |S_A|$ $\Rightarrow m(A_2) < m(A)$.
$|Q_2| = |Q|$

7.3.6. Voor elke toestandsautomaat $\mathcal{K}$ is er een cascadeprodukt van toestandsautomaten $\mathcal{K}_1$, $\mathcal{K}_2$, ... , $\mathcal{K}_h$, dat $\mathcal{K}$ realiseert en waarvoor geldt:
óf $\mathcal{K}_i$ is een permutatie-toestandsautomaat en $(S_{A_i},)|(S_A,)$,
óf $\mathcal{K}_i$ is een reset-toestandsautomaat met twee toestanden.

bewijs: Als $\mathcal{K}$ een permutatie-toestandsautomaat of een reset-toestandsautomaat met twee toestanden is, is het bewijs triviaal, evenals in het geval met $m(A)=(1,1,1)$, hetgeen het minimum is.
De hypothese is nu, dat de stelling waar is voor alle toestandsautomaten, waarvan de maat kleiner is als $m(A)$.
Dan is de stelling dus ook waar voor $\mathcal{K}_1$ en $\mathcal{K}_2$, die door 7.3.5. geleverd worden.
$\mathcal{K}_{1i}$ $(1 \leq i \leq n)$ zijn de toestandsautomaten in de cascade voor $\mathcal{K}_1$.
$\mathcal{K}_{2i}$ $(1 \leq i \leq m)$ zijn de toestandsautomaten in de cascade voor $\mathcal{K}_2$.
Volgens 6.3.8. en 6.3.10. realiseert een cascade van alle $\mathcal{K}_{1i}$ en alle $\mathcal{K}_{2i}$ dan ook $\mathcal{K}$.
Veronderstel nu, dat $(S_{A_{1i}},)$ een groep is, dan geldt volgens de hypothese dat $(S_{A_{1i}},)|(S_{A_1},)$.
Maar als een groep een monoïde $(S,)$ deelt, dan moet deze groep ook $(S*,)$ delen. Dus $(S_{A_{1i}},)|(S_{A_1}*,)$.
Volgens 7.3.5. : $(S_{A_1}*,)|(S_{A_1},)$
Ten slotte, volgens 4.1.20., $(S_{A_{1i}},)|(S_A,)$.
Voor $\mathcal{K}_2$ geldt hetzelfde.

7.3.7. Voor elke toestandsautomaat $\mathcal{K}$ bestaat er een cascádeprodukt van toestandsautomaten $\mathcal{K}_1$, $\mathcal{K}_2$, ... , $\mathcal{K}_n$, dat $\mathcal{K}$ realiseert, terwijl voor alle i $(1 \leq i \leq n)$ geldt:
óf $(S_{A_i},)$ is een enkelvoudige groep en $(S_{A_i},)|(S_A,)$,
óf $\mathcal{K}_i$ is een reset-toestandsautomaat met twee toestanden.

bewijs: Daar elke factor van de compositierij de oorspronkelijke groep deelt, volgt deze stelling direkt uit 7.3.6., 7.2.4. en 4.1.20.

8. Ontleding van een willekeurig toestandsautomaat

8.1. Opvolgers

8.1.1. C is een toelaatbare overdekking van Q met $\#C > 1$.
Twee blokken van C, B_i en B_j, noemen we verwant als
$\exists_{v \in X^*} \exists_{w \in X^*} [B_i \tau_v = B_j \wedge B_j \tau_w = B_i]$
Notatie: $B_i @ B_j$

8.1.2. De relatie 'verwant zijn' is een equivalentierelatie.

bewijs: $B_i \tau_\Lambda = B_i \Rightarrow B_i @ B_i \Rightarrow$ reflexiviteit.

$B_i @ B_j \Rightarrow \exists_{v \in X^*} \exists_{w \in X^*} [B_i \tau_v = B_j \wedge B_j \tau_w = B_i] \Rightarrow B_j @ B_i \Rightarrow$ symmetrie.

$B_i @ B_j \wedge B_j @ B_k \Rightarrow \exists_{v_1 \in X^*} \exists_{w_1 \in X^*} [B_i \tau_{v_1} = B_j \wedge B_j \tau_{w_1} = B_i] \wedge \exists_{v_2 \in X^*} \exists_{w_2 \in X^*} [B_j \tau_{v_2} = B_k \wedge B_k \tau_{w_2} = B_j] \Rightarrow$
$\Rightarrow B_i \tau_{v_1} \tau_{v_2} = B_k \wedge B_k \tau_{w_2} \tau_{w_1} = B_i \Rightarrow B_i @ B_k \Rightarrow$ transitiviteit.

8.1.3. $B_i @ B_j \Rightarrow |B_i| = |B_j|$

bewijs: $\left.\begin{array}{l} \tau_v \text{ is een afbeelding} \Rightarrow |B_i \tau_v| = |B_j| \leq |B_i| \\ \tau_w \text{ is een afbeelding} \Rightarrow |B_j \tau_w| = |B_i| \leq |B_j| \end{array}\right\} |B_i| = |B_j|$

8.1.4. C is een toelaatbare overdekking van Q met $\#C > 1$.
Een klasse van onderling verwante blokken van C heet initieel als elk blok in die klasse $\#C$ elementen bevat.
De blokken van een initiële klassen noemen we ook initieel.

8.1.5. C is een toelaatbare overdekking van Q en $\#C > 1$.
Voor alle K bestaat er een initiële klasse in C.

bewijs: Voor opdeling van C in klassen geldt:
elk blok bevindt zich in precies één klasse (8.1.2.)
Er is ten minste één blok in C met $\#C$ elementen. Uit 8.1.3. volgt dan dat de klasse van zo'n blok initieel is.

opm. Een overdekking kan meer als één initiële klasse bevatten.

8.1.6. C is een toelaatbare overdekking van Q met $\#C > 1$.
D is een initiële klasse van C.
De familie van deelverzamelingen van Q, die gedefinieerd is als
$(C \div D) + \sum_{B \in D} ASS(\{B'\tau_w \mid B' \in C \wedge w \in X^* \wedge B'\tau_w \subset B\} \cup \{\{q\} \mid q \in B\})$,
heet de opvolger van C.
Als $B_i \in D$, dan $\mathcal{P}_i := ASS(\{B'\tau_w \mid B' \in C \wedge w \in X^* \wedge B'\tau_w \subset B_i\} \cup \{\{q\} \mid q \in B_i\})$.
$\alpha_i := |\mathcal{P}_i|$.

8.1.7. C is een toelaatbare overdekking van Q met $\#C > 1$.
Elke opvolger van C is een toelaatbare overdekking van Q die echt fijner is als C.

bewijs: De opvolger is een overdekking. Immers alle elementen van Q die niet in D voorkomen, komen in $(C \div D)$ voor. Elk element van $B_i \in D$ komt in $\{\{q\} \mid q \in B_i\}$ voor en dus in het verzamelingensysteem $\mathcal{P}_i$. Dit geldt voor alle $B \in D$.
De opvolger is echt fijner, want elke $B \in D$ is vervangen door echte deelverzamelingen van B. Uit de definitie van deze nieuwe blokken volgt ook dat de opvolger van C weer toelaatbaar is.

8.1.8. C is een toelaatbare overdekking van Q met $\#C > 1$.
D is een initiële klasse van C.
$\forall_{B_i \in D} [\alpha_i = \alpha_1]$.

bewijs: We geven de blokken van $\mathcal{P}_i$ aan met $B'_{i1}, B'_{i2}, \ldots, B'_{i\alpha_i}$.
$\left.\begin{matrix} B_1 \in D \\ B_i \in D \end{matrix}\right\} \Rightarrow B_1 \mathbin{@} B_i \Rightarrow \exists_{\omega_i \in X^*} [B_i \tau_{\omega_i} = B_1] \wedge \exists_{\nu_i \in X^*} [B_1 \tau_{\nu_i} = B_i] \Rightarrow B_1 \tau_{\nu_i} \tau_{\omega_i} = B_1 \Rightarrow$
$\Rightarrow D_{B_1} \tau_{\nu_i} \tau_{\omega_i}$ is een permutatie van $B_1 \Rightarrow \exists_{r \in \mathbb{N}} \forall_{q \in B_1} [q (\tau_{\nu_i} \tau_{\omega_i})^r = q]$

We bekijken nu de surjectieve afbeelding $(\tau_{\nu_i} \tau_{\omega_i})^{r-1} \tau_{\nu_i}$. Deze beeldt B_1 op B_i af. Het blok B'_{1p} wordt er door in B'_{iq} afgebeeld:
$B'_{ip} = B'_{1p} (\tau_{\nu_i} \tau_{\omega_i})^r = B'_{1p} (\tau_{\nu_i} \tau_{\omega_i})^{r-1} \tau_{\nu_i} \tau_{\omega_i} \subseteq B'_{iq} \tau_{\omega_i}$.
τ_{ω_i} beeldt B_i op B_1 af, dwz. $\exists_{B'_{iu} \in \mathcal{P}'} [B'_{iq} \tau_{\omega_i} \subseteq B'_{iu}]$.
Daar $\mathcal{P}_i$ een verzamelingensysteem is moet dan $B'_{ip} = B'_{iu} = B'_{iq} \tau_{\omega_i}$.
$D_{B'_{ip}} (\tau_{\nu_i} \tau_{\omega_i})^{r-1} \tau_{\nu_i}$ en $D_{B'_{iq}} \tau_{\omega_i}$ zijn een-eenduidig en $|B'_{ip}| = |B'_{iq}|$ en $B'_{ip} (\tau_{\nu_i} \tau_{\omega_i})^{r-1} \tau_{\nu_i} = B'_{iq}$.

Stel nu $B'_{is} \neq B'_{ip}$. Er is een t, zodat $B'_{is} (\tau_{\nu_i} \tau_{\omega_i})^{r-1} \tau_{\nu_i} = B'_{it}$.
Nu moet gelden dat $B'_{it} \neq B'_{iq}$, want $B'_{iq} \tau_{\omega_i} = B'_{ip}$ en $B'_{it} \tau_{\omega_i} = B'_{is}$. Als dus $B'_{it} = B'_{iq}$, dan zou ook $B'_{ip} = B'_{is}$, hetgeen in strijd is met onze aanname.

Conclusie: verschillende blokken in $\mathcal{P}_1$ worden op verschillende blokken in $\mathcal{P}_i$ afgebeeld.

Op analoge wijze bewijst men dat verschillende blokken van $\mathcal{P}_i$ op verschillende blokken in $\mathcal{P}_1$ worden afgebeeld.

Dus $\alpha_1 = \alpha_i$.

8.1.9. C is een toelaatbare overdekking van Q met $\#C > 1$.
C' is een opvolger van C.
We plaatsen nu de elementen van C' in het zgn. opvolgerstableau:

	k_1	k_2	k_3	$\ldots$	k_α
r_1	B'_{11}	B'_{12}	B'_{13}	$\ldots$	$B'_{1\alpha}$
r_2	B'_{21}	B'_{22}	B'_{23}	$\ldots$	$B'_{2\alpha}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
r_m	B'_{m1}	B'_{m2}	B'_{m3}	$\ldots$	$B'_{m\alpha}$
r_{m+1}	B'_{m+1}				
r_{m+2}	B'_{m+2}				
$\vdots$	$\vdots$				
r_t	B'_t				

Hierin is: $\alpha = \alpha_1$,
$B'_{ip} = B'_{1p} (\tau_{\nu_i} \tau_{\omega_i})^{r-1} \tau_{\nu_i}$ en dus ook $B'_{ip} \tau_{\omega_i} = B'_{1p}$,
$B'_{m+i} = B_{m+j}$.

8.1.10. C is een toelaatbare overdekking van Q met $\#C > 1$.
D is een initiële klasse van C
Als er een $x \in X$ is, zodat τ_x $B_i \in D$ op $B_j \in D$ afbeeldt ($B_i \tau_x = B_j$), dan definiëren we een permutatie γ_x^{ij} over de getallen 1, 2, $\ldots$, α:
$B'_{ip} \tau_x = B'_{jq} \Leftrightarrow p \gamma_x^{ij} = q$.

8.1.11. De afbeelding $(\tau_{\nu_i} \tau_{\omega_i})^{r-1} \tau_{\nu_i} \tau_x \tau_{\omega_i}$ permuteert de blokken van $\mathcal{P}_1$ precies zo als γ_x^{ij} de tweede indices.

bewijs: $B'_{1p} (\tau_{\nu_i} \tau_{\omega_i})^{r-1} \tau_{\nu_i} \tau_x \tau_{\omega_i} = B'_{ip} \tau_x \tau_{\omega_i} = B'_{i\,p\,\gamma_x^{ij}} \tau_{\omega_i} = B'_{1\,p\,\gamma_x^{ij}}$.

8.1.12. C is een toelaatbare overdekking van Q met $\#C > 1$.
C' is een opvolger van C.
De blokken van C', beschouwd als toestanden van een C'-factor A' van A, vormen een verzameling Q'
μ_k is de partitie met als blokken de kolommen van het opvolgerstableau.
μ_r is de partitie met als blokken de rijen van het opvolgerstableau.

8.1.13. C is een toelaatbare overdekking van Q met $\#C > 1$.
C' is een opvolger van C.
Er bestaat een C'-factor A' van A, zodat μ_r een toelaatbare partitie van A' is en $A'/\mu_r \simeq A/C$

bewijs: We geven A/C aan met A''.
We constateren dat de vereniging van de elementen van een blok van μ_r een blok van C is.

Stel nu $B_i \in C \wedge B_i\tau_x \notin D \wedge \underline{B}_i\tau''_x = \underline{B}_j$.
Dit betekent dat $B_i\tau_x \subseteq B_j$. Er moet dus een blok van C' in de rij j van het tableau staan, dat $B_i\tau_x$ geheel bevat. We geven dit blok aan met B'.
We definiëren τ'_x in zo'n geval als volgt:
$i \leq m$: $\underline{B}'_{ip}\tau'_x = \underline{B}'$ ongeacht p
$i > m$ $\underline{B}'_i\tau'_x = \underline{B}'$.

Stel nu $B_i \in C \wedge B_i\tau_x = B_j \in D$.
Dit betekent dat $B_i \in D$ en $\underline{B}_i\tau''_x = \underline{B}_j$ (dus $i \leq m$).
In dit geval definiëren we τ'_x als $\underline{B}'_{ip}\tau'_x = \underline{B}'_{jp}\gamma^{ij}_x$

τ'_x is nu zo gedefinieerd, dat de eerste index aangeeft in welk blok van C we zitten, oftewel in welke rij van het tableau, oftewel in welk blok van μ_r.
μ_r is dus toelaatbaar en $A'/\mu_r \simeq A/C$

8.1.14. C is een toelaatbare overdekking van Q met $\#C > 1$.
C' is een opvolger van C.
De C'-factor A' van A kan als cascadeprodukt $A_1 \ominus A_2$ gerealiseerd worden, waarbij A_1 dan isomorf is met A/C en A_2 een permutatie-reset-toestands-automaat is.

bewijs: Uit 6.3.11. volgt, dat er een cascade $A_1 \ominus A_2$ bestaat, die A' realiseert met $A_1 \simeq A'/\mu_r \simeq A/C$. Verder heeft A_2 dan de toestandsverzameling μ_k.
We moeten nu nog laten zien, dat A_2 een permutatie-reset-toestandsautomaat is.
$Q_1 = \{r_1, r_2, \ldots, r_t\}$; $Q_2 = \{k_1, k_2, \ldots, k_\alpha\}$.
π_k is een gemodificeerde natuurlijke afbeelding: $B'\pi_k = k_i \Leftrightarrow B'$ is in kolom i.
$k_l\tau^2_{(r_i,x)} = \underline{B}'_{il}\tau'_x\pi_k$ is dan een definitie voor $\tau^2_{(r_i,x)}$, als men voor $i > m$ B'_{il} opvat als B'_j.
Daarom voor $i > m$: $k_l\tau^2_{(r_i,x)} = k_1\tau^2_{(r_i,x)}$ voor alle $1 \leq l \leq \alpha$, dwz. $\tau^2_{(r_i,x)}$ is dan een reset!
We moeten nu nog bewijzen dat $\tau^2_{(r_i,x)}$ voor $i \leq m$ een reset of een permutatie is.
Stel eerst $B_i\tau_x \notin D$. Volgens de constructie van A' in 8.1.13. hangt $\underline{B}'_{il}\tau'_x$ niet van l af, dus ook $k_l\tau^2_{(r_i,x)}$ hangt niet van l af $\Rightarrow$ $\tau^2_{(r_i,x)}$ is ook in dit geval een reset!
Nu het laatste geval: $B_i\tau_x = B_j \in D$. Weer volgens 8.1.13.:
$\underline{B}'_{il}\tau'_x = \underline{B}'_{jl}\gamma^{ij}_x \Rightarrow k_l\tau^2_{(r_i,x)} = B'_{jl}\gamma^{ij}_x\pi_k = k_{l\gamma^{ij}_x}$, een permutatie dus.

8.1.15. De groep $(G_2,)$ die gegenereerd wordt door de permutaties in A_2', deelt de semigroep $(S_A,)$.

bewijs: Uit 8.1.11. volgt, dat met elke permutatie in A_2' een $w \in X^*$ correspondeert, zodat τ_w' de blokken $B_{11}', B_{12}', \ldots, B_{1\alpha}'$ op precies dezelfde wijze permuteert. De groep $(G,)$ door deze permutaties gegenereerd is dus isomorf met $(G_2,)$.

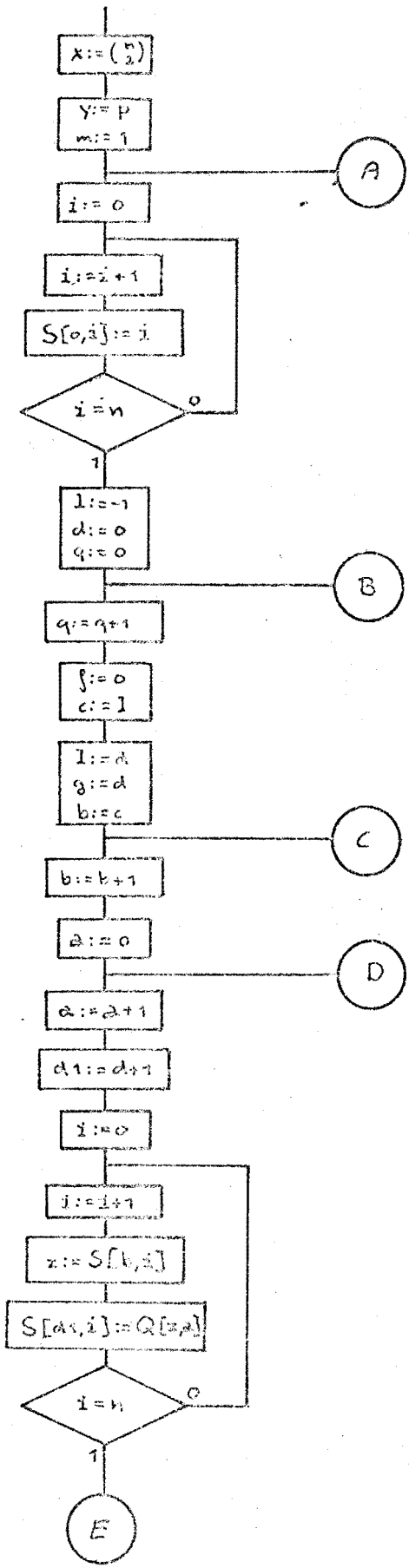
$Z := Q \cup \beta_1$. Als $D_{\beta_1}\tau_w'$ een permutatie over β_1 is, dan definiëren we

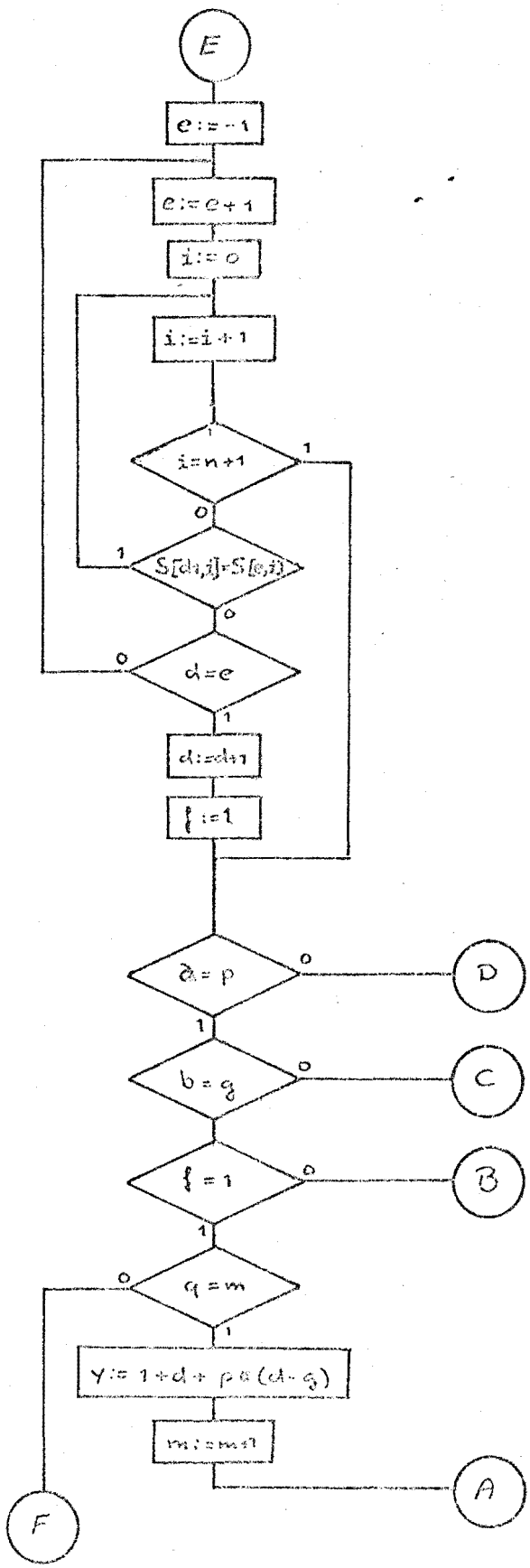
$$z\bar{\tau}_w = \begin{cases} z\tau_w & \text{als } z \in Q \\ z\tau_w' & \text{als } z \in \beta_1 \end{cases}$$

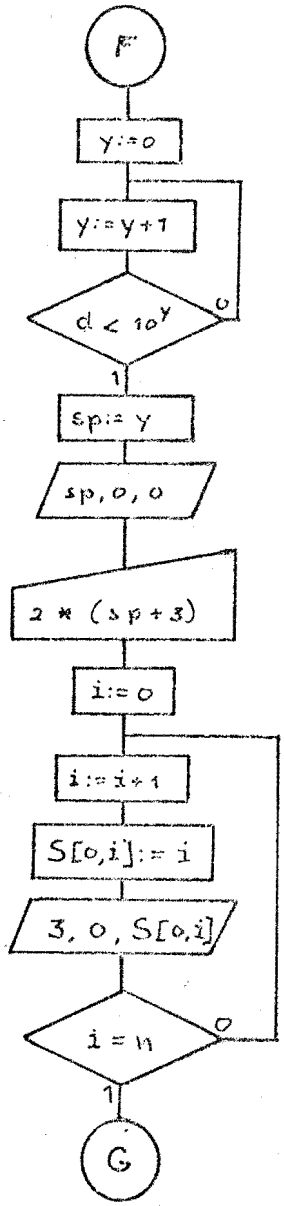
Daar $(\bar{\tau}_{w_1} = \bar{\tau}_{w_2} \Leftrightarrow \tau_{w_1} = \tau_{w_2})$, is de ondersemigroep $(T_A,)$ van $(S_A,)$, die gegenereerd wordt door $\{\tau_w \mid |\beta_1\tau_w'| = |\beta_1|\}$ isomorf met de semigroep $(\bar{T},)$ met $\bar{T} = \langle \{\bar{\tau}_w \mid |\beta_1\tau_w'| = |\beta_1|\} \rangle$.

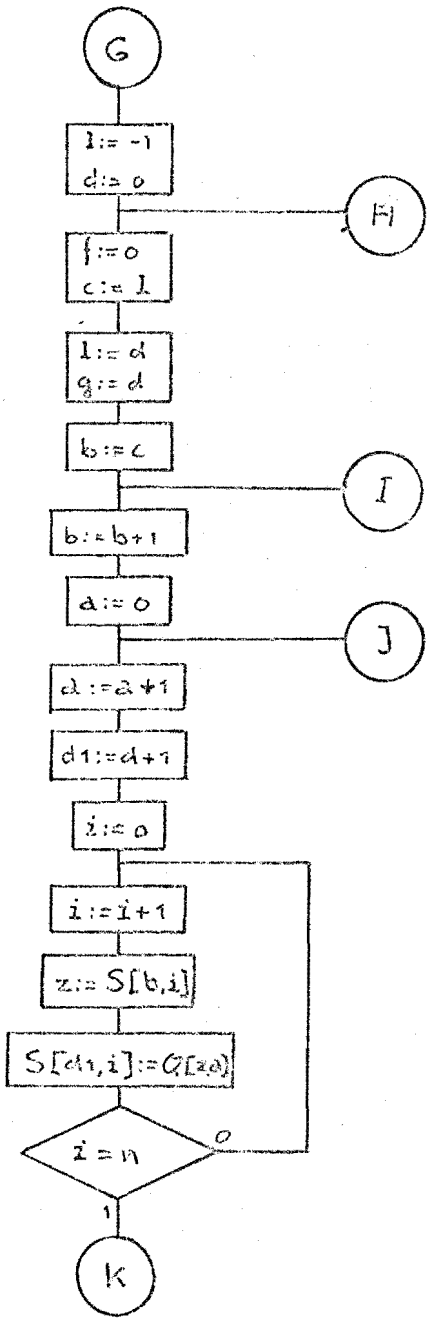
Volgens 4.3.6. geldt nu $\left.\begin{array}{l}(G,) \mid (\bar{T},) \\ (\bar{T},) \simeq (T_A,) \mid (S_A,)\end{array}\right\} \Rightarrow (G,) \mid (S_A,)$

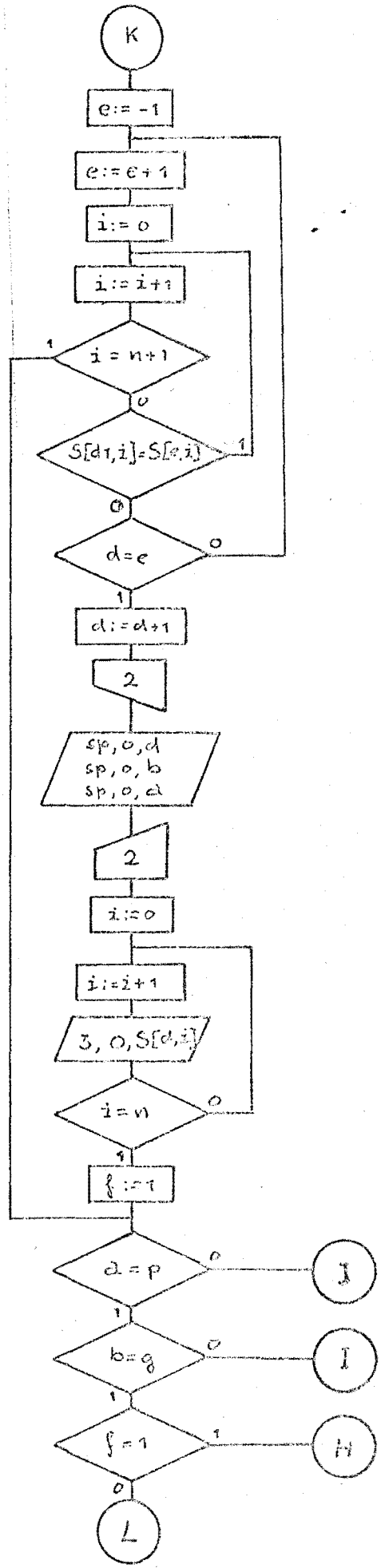
Verder $\left.\begin{array}{l}(G,) \mid (S_A,) \\ (G_2,) \simeq (G,)\end{array}\right\} \Rightarrow (G_2,) \mid (S_A,).$

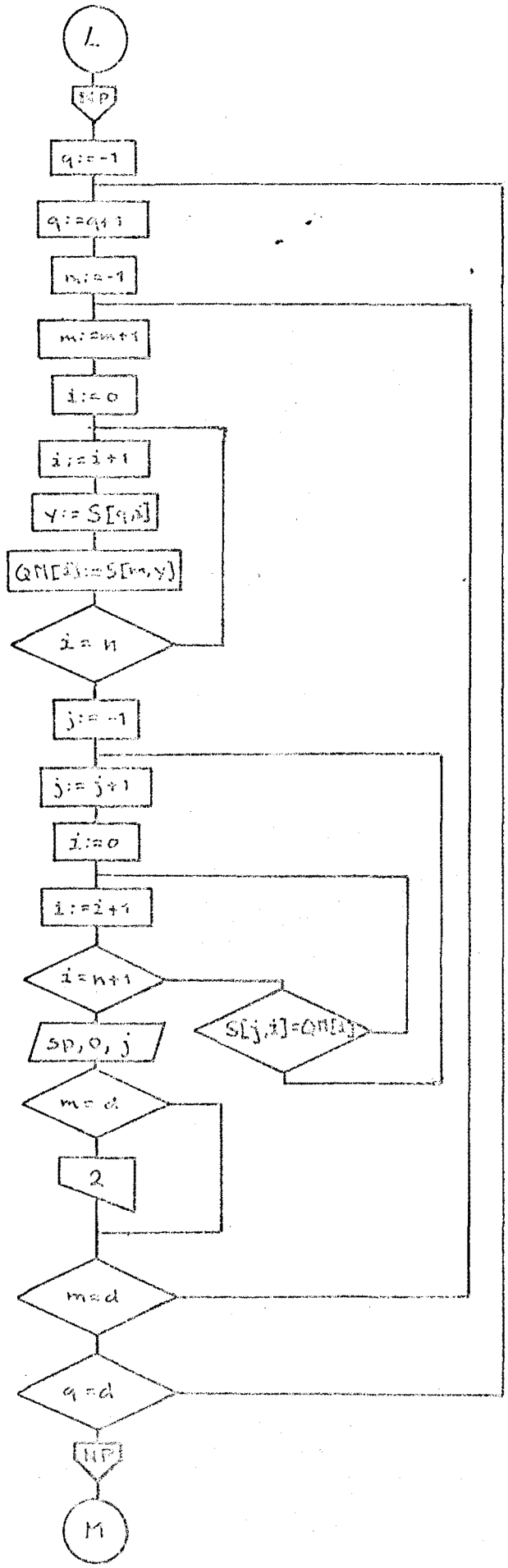

x:=(n 2)
Y:=P
m:=1
A
i:=0
i:=i+1
S[0,i]:=i
i=n
0
1
l:=-1
d:=0
q:=0
B
q:=q+1
f:=0
c:=1
l:=d
g:=d
b:=c
C
b:=b+1
a:=0
D
a:=a+1
d1:=d+1
i:=0
j:=i+1
x:=S[l,j]
S[d1,i]:=Q[x,d]
i=n
0
1
E

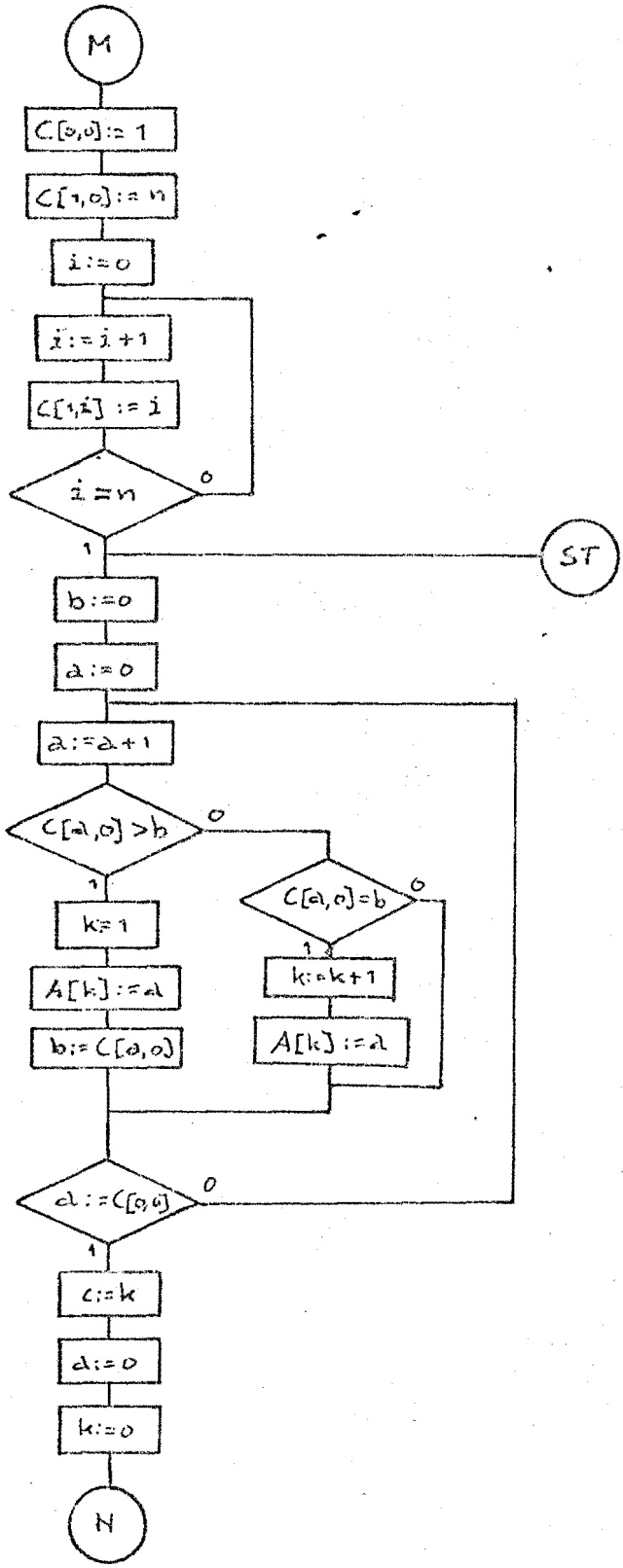

E
e:=-1
e:=e+1
i:=0
i:=i+1
i=n+1
1
0
S[d,j]=S[e,j]
1
0
d=e
0
1
d:=d+1
f:=1
a=p
0
D
1
b=g
0
C
f=1
0
B
1
q=m
0
1
y:=1+d+p*(d-q)
m:=m+1
A
F

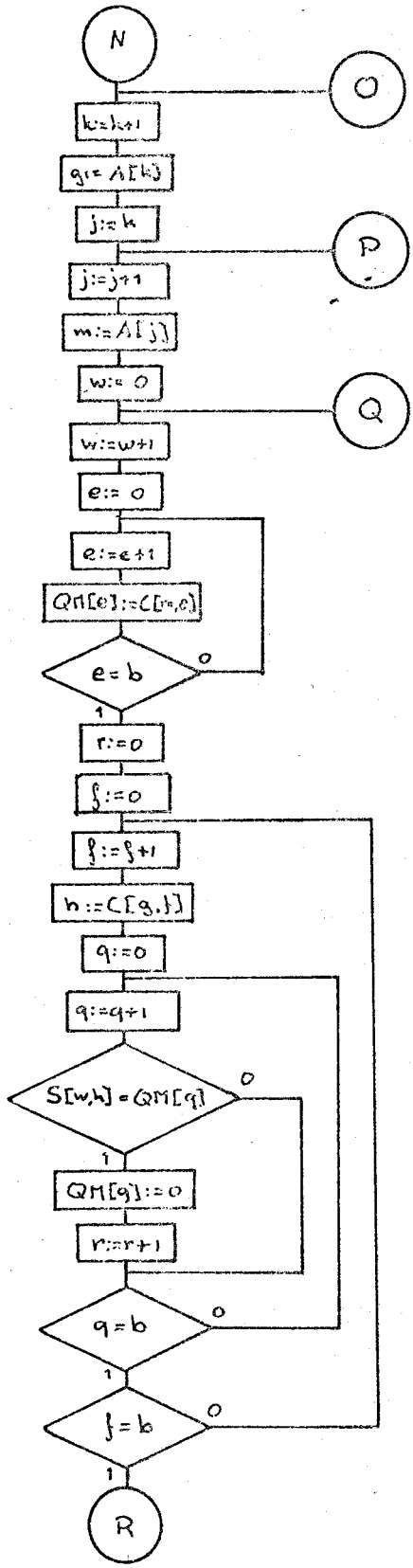

F
y:=0
y:=y+1
d < 10^y
0
1
sp:= y
sp, 0, 0
2 * (sp+3)
i:= 0
i:= i+1
S[0,i]:= i
3, 0, S[0,i]
i = n
0
1
G

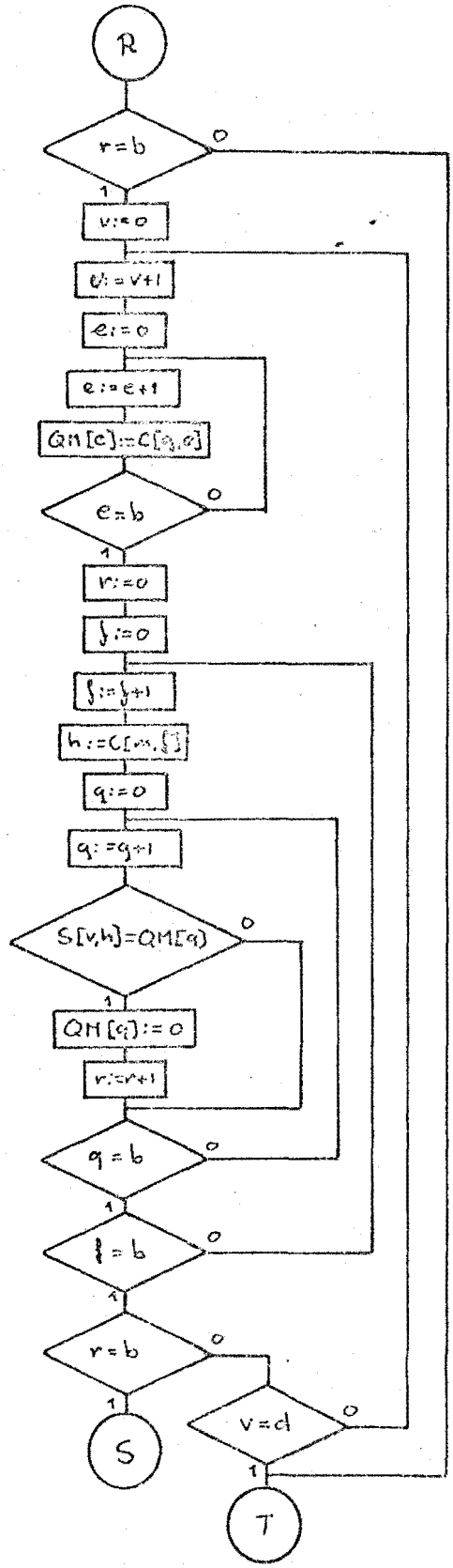

G
l:= -1
d:= 0
H
f:=0
c:= l
l:= d
g:= d
b:=c
I
b:=b+1
a:= 0
J
d:=a+1
d1:=d+1
i:= 0
i:=i+1
z:= S[b,i]
S[d1,i]:=Q[za]
i = n
0
1
K

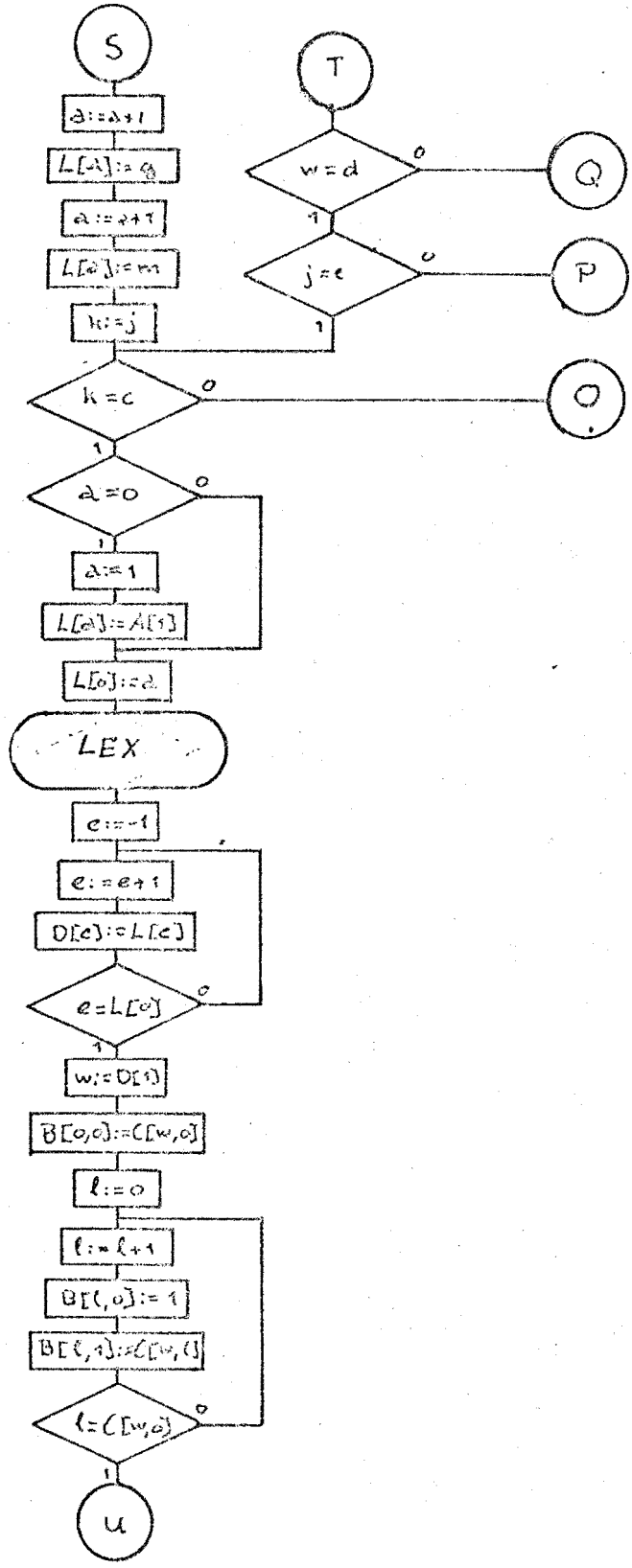

K
e:= -1
e:=e+1
i:= 0
i:=i+1
i = n+1
S[d1,i]=S[e,i]
d=e
d:=d+1
2
sp, 0, d
sp, 0, b
sp, 0, a
2
i:=0
i:=i+1
3, 0, S[d,i]
i=n
f:=1
d=p
b=g
f=1
J
I
H
L


L
INP
q:=-1
q:=q+1
m:=-1
m:=m+1
i:=0
i:=i+1
y:=S[q,i]
QN[i]:=S[m,y]
i=n
j:=-1
j:=j+1
i:=0
i:=i+1
i=n+1
S[j,i]=QN[i]
sp,0,j
m=d
2
m=d
q=d
INP
M


M
C[0,0]:= 1
C[1,0]:= n
i:=0
i:=i+1
C[1,i]:= i
i=n
0
1
ST
b:=0
a:=0
a:=a+1
C[a,0]>b
0
1
C[a,0]=b
0
1
k:=1
A[k]:=a
b:=C[a,0]
k:=k+1
A[k]:=a
a:=C[0,0]
0
1
c:=k
d:=0
k:=0
N


N
O
k:=k+1
q:= A[k]
j:= k
P
j:=j+1
m:=A[j]
w:= 0
Q
w:=w+1
e:= 0
e:=e+1
QM[e]:=C[m,e]
e=b
0
1
r:=0
f:=0
f:=f+1
h:=C[q,f]
q:=0
q:=q+1
S[w,h]=QM[q]
0
1
QM[q]:=0
r:=r+1
q=b
0
1
f=b
0
1
R


R
r=b
0
1
v:=0
v:=v+1
e:=0
e:=e+1
QM[e]:=C[v,e]
e=b
0
1
r:=0
f:=0
f:=f+1
h:=C[r,f]
q:=0
q:=q+1
S[v,h]=QM[q]
0
1
QM[q]:=0
r:=r+1
q=b
0
1
f=b
0
1
r=b
0
1
v=d
0
1
S
T


S
a:=a+1
L[a]:=q
a:=a+1
L[a]:=m
k:=j
k=c
a=0
a:=1
L[a]:=A[1]
L[a]:=a
LEX
e:=-1
e:=e+1
D[e]:=L[e]
e=L[e]
w:=D[1]
B[0,0]:=C[w,0]
l:=0
l:=l+1
B[l,0]:=1
B[l,1]:=C[w,l]
l=C[w,0]
U
T
w=d
j=c
Q
P
O

9. Onontleedbaarheid

9.1.1. Een toestandsautomaat $\mathcal{A}$ heet onontleedbaar als voor elke cascade $\mathcal{A}_1 \textcircled{\omega} \mathcal{A}_2$ die $\mathcal{A}$ realiseert, geldt:
$(S_A, \ ) \mid (S_{A_1}, \ ) \vee (S_A, \ ) \mid (S_{A_2}, \ )$.

9.1.2. $\mathcal{A}_0 = \mathcal{A}_1 \textcircled{\omega} \mathcal{A}_2 \geq \mathcal{A}$.
$(G, \ )$ is een enkelvoudige groep en $(G, \ ) \mid (S_A, \ )$.
Dan geldt
$(G, \ ) \mid (S_{A_1}, \ ) \vee (G, \ ) \mid (S_{A_2}, \ )$.

bewijs: We geven eerst een expliciete uitdrukking van de toestandsveranderingen in de cascade $\mathcal{A}_1 \textcircled{\omega} \mathcal{A}_2$.
$w \in X^*$ en $w = x_1 x_2 x_3 \ldots x_{k-1}$.

$$\begin{aligned}(q_1, q_2)\tau^o_{wx_k} &= (q_1, q_2)\tau^o_{x_1}\tau^o_{x_2} \ldots \tau^o_{x_k} = \\ &= (q_1 \tau^1_{x_1}, q_2 \tau^2_{(q_1, x_1)\omega})\tau^o_{x_2}\tau^o_{x_3} \ldots \tau^o_{x_k} = \\ &= (q_1 \tau^1_{x_1 x_2}, q_2 \tau^2_{(q_1, x_1)\omega}\tau^2_{(q_1\tau^1_{x_1}, x_2)\omega})\tau^o_{x_3}\tau^o_{x_4} \ldots \tau^o_{x_k} = \\ &= \ldots\ldots\ldots\ldots\ldots\ldots = \\ &= (q_1 \tau^1_{wx_k}, q_2 \tau^2_{(q_1, x_1)\omega}\tau^2_{(q_1\tau^1_{x_1}, x_2)\omega}\tau^2_{(q_1\tau^1_{x_1 x_2}, x_3)\omega} \ldots \tau^2_{(q_1\tau^1_{w}, x_k)\omega})\end{aligned}$$

Door gebruik van diverse stellingen laat zich het bewijs als volgt opschrijven:

$$\left.\begin{array}{l}(S_A, \ ) \mid (S_{A_0}, \ ) \quad (6.1.13) \\ (G, \ ) \mid (S_A, \ )\end{array}\right\} \Rightarrow (G, \ ) \mid (S_{A_0}, \ ) \quad (4.1.20)$$

dwz. $(G, \ )$ is een homomorf beeld van een ondergroep $(H, \ )$ van $(S_{A_0}, \ )$ (4.3.4).

Volgens 4.3.5. kunnen we een $W \subset Q_1 \times Q_2$ vinden, zodat
$\tau^o_x \in H \Rightarrow (Q_1 \times Q_2) D_W \tau^o_x = (Q_1 \times Q_2) D_W$ en $(\langle \{\tau^o_x D_W \mid \tau^o_x \in H\} \rangle, \ ) \simeq (H, \ )$.

$W_1 = \{q_1 \mid (q_1, q_2) \in W\}$
$H_o = \{\tau^o_w \mid \tau^o_w \in H \wedge \tau^1_w = D_{W_1}\}$.

$H_o \neq \emptyset$, omdat de identiteit van H een element van H_o is.

$$\left.\begin{array}{l}\text{Het is duidelijk dat } (H_o, \ ) \lhd (H, \ ) \\ \text{Bovendien } \forall_{\tau^o_w \in H} \left[(\tau^o_w)^{-1} H_o (\tau^o_w) = H_o\right]\end{array}\right\} \Rightarrow (H_o, \ ) \lll (H, \ ) \quad (4.2.25)$$

Volgens 4.2.16. zitten τ^o_w en τ^o_v van H slechts in dezelfde nevenklasse van H als $\tau^o_w (\tau^o_v)^{-1} \in H_o$; dit betekent dat $D_{W_1} (\tau^1_{wx})(\tau^1_v)^{-1} = D_{W_1}$.
Een nevenklasse van H_o wordt dus gevormd door die elementen van H, die op W_1 precies gelijk werken: $D_{W_1}\tau^1_w = D_{W_1}\tau^1_v$.
Dwz. $(\langle \{\tau^1_w D_{W_1} \mid \tau^o_w \in H_o\} \rangle, \ ) \simeq (H/H_o, \ )$ en dus volgens 4.3.6. :
$(H/H_o, \ ) \mid (S_{A_1}, \ )$.

We definiëren weer twee toestandsverzamelingen:
$W_{q_1} = \{(q_1, q_2) \mid (q_1, q_2) \in W\}$
$U_{q_1} = \{q_2 \mid (q_1, q_2) \in W_{q_1}\}$
Als $\tau^o_{wx_k} \in H_o$, dan $(q_1, q_2)\tau^o_{wx_k} = (q_1 \tau^1_{wx_k}, q_2 \tau^{2^{q_1}}_{wq_1 x_k})$ met
$\tau^{2^{q_1}}_{wx_k} = \tau^2_{(q_1, x_1)\omega}\tau^2_{(q_1\tau^1_{x_1}, x_2)}\tau^2_{(q_1\tau^1_{x_1}\tau^1_{x_2}, x_3)\omega} \ldots \tau^2_{(q_1\tau^1_w, x_k)\omega}$
$\tau^o_{wx_k}$ permuteert de elementen van W $\Rightarrow$ $\tau^{2^{q_1}}_{wx_k} D_{U_{q_1}}$ is een permutatie over $U_{q_1} \subset Q_2$
$q_1 \tau^1_{wx_k} = q_1$

We concluderen hieruit:
De restrictie van elementen van H_o tot W_{q_1} vormt een groep $(H_{q_1}, \ )$ die isomorf is met $(\langle \{\tau^1_{wx_k} D_{U_{q_1}} \mid \tau^o_{wx_k} \in H_o\} \rangle, \ )$ en deze laatste groep is volgens 4.3.6. een homomorf beeld van een ondergroep van $(S_{A_2}, \ )$.

Bovenstaande conclusie geldt voor elk element van W_1, en zo verkrijgen we $|W_1|=v$ groepen: $(H_{q_1^{(\omega)}},)$, $(H_{q_1^{(\omega)}},)$, ... , $(H_{q_1^{(\omega)}},)$. Verder is $\{W_{q_1^{(\omega)}}, W_{q_1^{(\omega)}}, \ldots, W_{q_1^{(\omega)}}\}$ een partitie op W.
Uit dit alles volgt: $\tau^{\circ}_{\omega x_k} \in H_o \Rightarrow \tau^{\circ}_{\omega x_k} D_W \in (H_{q_1^{(\omega)}} x H_{q_1^{(\omega)}} x \ldots\ldots x H_{q_1^{(\omega)}},)$.
Volgens 4.3.5. geldt ook dat deze $\tau^{\circ}_{\omega x_k} D_W$ tezamen een groep vormen isomorf met H_o.
Dus $(H_o,) \simeq (K,) \lhd (H_{q_1^{(\omega)}} x H_{q_1^{(\omega)}} x \ldots\ldots x H_{q_1^{(\omega)}},)$

Mbv. 4.2.52. zien we dan, daar $(G,) | (H,)$, dat $(G,) | (H/H_o,)$ & $(G,) | (H_o,)$.

Hiermee is de stelling bewezen, want
als $(G,) | (H/H_o,)$, dan volgt uit het feit dat $(H/H_o,) | (S_{A_1},)$, $(G,) | (S_{A_1},)$
en als $(G,) | (H_o,)$, dan volgt uit een generalisatie van 4.2.58. :
$\left.\begin{array}{l} \exists_{q_1 \in W_1} [(H_o,) | (H_{q_1},)] \\ \forall_{q_1 \in W_1} [(H_{q_1},) | (S_{A_2},)] \end{array}\right\} \Rightarrow (G,) | (S_{A_2},)$.

9.1.3. Als $\mathcal{K}$ een resettoestandsautomaat met twee toestanden is, dan is $(S_A,)$ isomorf met een van de volgende drie semigroepen:
$(\{e\},)$,
$(S_1,) = (\{\tau_o, \tau_1\},)$ met $\tau_i\tau_o = \tau_i$ en $\tau_i\tau_1 = \tau_1$, $(i = o,1)$
$(S_2,) = (\{\tau_o, \tau_1, \tau_2\},)$ met $\tau_i\tau_o = \tau_i$, $\tau_i\tau_1 = \tau_1$ en $\tau_i\tau_2 = \tau_2$. $(i = o,1,2)$

bewijs: Ga alle mogelijkheden na!

9.1.4. Als $(T,)$ een eindige semigroep is en $(S_2,) | (T,)$, dan is er een ondersemigroep van $(T,)$ die isomorf is met $(S_2,)$.

bewijs: φ is het homomorfisme uit T op S_2.
$(\tau_o \varphi^{-1},)$ is een ondersemigroep van $(T,)$.
Uit 4.3.3. weten we dat er dan een idempotent element e in $\tau_o\varphi^{-1}$ is.
We definiëren $T' = eTe$. Dan is $(T',)$ een ondermonoïde van $(T,)$ met e als eenheid (zie bewijs 4.3.4.).
$\varphi' = D_T \varphi$, dan
$$T'\varphi' = T'\varphi = (eTe)\varphi = (e\varphi)(T\varphi)(e\varphi) = \tau_o S_2 \tau_o = S_2.$$
Dwz. φ' is een homomorfisme van T' op S_2.

Zij $(T'',)$ de minimale ondersemigroep van T', zodat $T''\varphi' = \{\tau_1, \tau_2\}$.
(Dit kunnen we eisen; immers $(\{\tau_1, \tau_2\},)$ is een ondersemigroep van S_2, dus $(\{\tau_1, \tau_2\}\varphi'^{-1},)$ is een ondersemigroep van $(T',)$; er bestaat dus ook een minimale ondersemigroep die aan de eisen voldoet.)

Voor elke $x \in T''$ is $(xT'',)$ een ondersemigroep van $(T'',)$, daar $xt_1''xt_2'' = x(t_1''xt_2'') \in xT''$. Zelfs geldt $xT'' = T''$, want T'' is minimaal en $xT''\varphi' = x\varphi' T''\varphi' = x\varphi'\{\tau_1, \tau_2\}$ en uit de definitie van $(S_2,)$ weten we dat $\tau_i\tau_1 = \tau_1$ en $\tau_i\tau_2 = \tau_2$.

Tot slot constateren we dat $(\tau_1\varphi'^{-1} \cap T'',)$ en $(\tau_2\varphi'^{-1} \cap T'',)$ twee niet-lege disjuncte ondersemigroepen van $(T'',)$ zijn. Beide hebben dus een idempotent element: f_1 resp f_2. Hiervoor geldt:
$f_1T'' = T'' \Rightarrow \exists_{u \in T''} [f_1u = f_2] \Rightarrow f_1f_2 = f_1f_2u = f_1u = f_2$.
$f_2T'' = T'' \Rightarrow \exists_{v \in T''} [f_2v = f_1] \Rightarrow f_2f_1 = f_2f_2v = f_2v = f_1$.
$(\{e, f_1, f_2\},)$ is een ondersemigroep van $(T',)$ en dus van $(T,)$ én is isomorf met $(S_2,)$.

9.1.5. Als $(T, \ )$ een eindige semigroep en $(S_1, \ ) \ (T, \ )$, dan is er een ondersemigroep van $(T, \ )$ die isomorf is met $(S_1, \ )$.

bewijs: φ is het homomorfisme uit T op S_1.
$(\tau_0\varphi^{-1}, \ )$ is een ondersemigroep van $(T, \ )$ met een idempotent element e.
$T'=eTe$; $(T', \ )$ is een ondermonoïde van $(T, \ )$ met e als eenheid.
$\varphi' = D_T \varphi$ is een homomorfisme van T' op S_1.
$(\{\tau_\lambda\}, \ )$ is een ondersemigroep van $(S_1, \ ) \Rightarrow (T''=\tau_\lambda\varphi^{-1}, \ )$ is een ondersemigroep van $(T', \ )$.
Er is een idempotent element f in T''.
$(\{e,f\}, \ )$ is een ondersemigroep van $(T', \ )$ en dus ook van $(T, \ )$ én is isomorf met $(S_1, \ )$.

9.1.6. $\aleph_0=\aleph_1 \textcircled{\omega} \aleph_2 \geq \aleph$
$(S_2, \ ) \mid (S_A, \ ) \Rightarrow (S_2, \ ) \mid (S_{A_1}, \ ) \vee (S_2, \ ) \ (S_{A_2}, \ )$.

bewijs: $\left.\begin{matrix}(S_A, \ ) \mid (S_{A_0}, \ ) \\ (S_2, \ ) \mid (S_A, \ )\end{matrix}\right\} \overset{(6.1.13)}{\Rightarrow} (S_2, \ ) \mid (S_{A_0}, \ )$

$$\exists_{\nu,\omega\in X^*}\left[\{\tau_\lambda^0, \tau_\nu^0, \tau_\omega^0\} \leq S_{A_0} \wedge (\{\tau_\lambda^0, \tau_\nu^0, \tau_\omega^0\}, \ ) \simeq (S, \ )\right.$$
$$\tau_\nu^0 \neq \tau_\omega^0 \Rightarrow \exists_{(q_1,q_2)\in Q_0}\left[(q_1', q_2') = (q_1, q_2)\tau_\nu^0 \neq (q_1, q_2)\tau_\omega^0 = (q_1'', q_2'')\right]$$

Uit 9.1.3. volgt:
$(q_1', q_2')\tau_\nu^0 = (q_1, q_2)\tau_\nu^0\tau_\nu^0 = (q_1, q_2)\tau_\nu^0 = (q_1', q_2')$
$(q_1', q_2')\tau_\omega^0 = (q_1, q_2)\tau_\nu^0\tau_\omega^0 = (q_1, q_2)\tau_\omega^0 = (q_1'', q_2'')$
$(q_1'', q_2'')\tau_\nu^0 = (q_1, q_2)\tau_\omega^0\tau_\nu^0 = (q_1, q_2)\tau_\omega^0 = (q_1'', q_2'')$
$(q_1'', q_2'')\tau_\omega^0 = (q_1, q_2)\tau_\omega^0\tau_\omega^0 = (q_1, q_2)\tau_\omega^0 = (q_1'', q_2'')$

We onderscheiden nu twee gevallen:
1. $\left.\begin{matrix}q_1' \neq q_2'' \Rightarrow q_1'\tau_\nu' = q_1' \wedge q_1'\tau_\omega' = q_1'' \Rightarrow \tau_\nu' \neq \tau_\omega' \\ \forall_{\nu',\omega',\mu'\in X^*}\left[\tau_\nu^0\tau_\omega^0 = \tau_\omega^0 \Rightarrow \tau_\nu'\tau_\omega' = \tau_\mu'\right]\end{matrix}\right\} \Rightarrow (\{\tau_\lambda', \tau_\omega', \tau_\nu'\}, \ ) \simeq (S_2, \ ) \Rightarrow$
$\Rightarrow (S_2, \ ) \mid (S_{A_1}, \ )$

2. $q_1' = q_1'' \Rightarrow q_2' \neq q_2''$
$\tau_\omega^{2^{q_1}} = \tau^2_{(q_1,x_1)\omega}\tau^2_{(q_1\tau'_{x_1}, x_2)} \cdots \tau^2_{(q_1\tau'_{x_1x_2}\cdots x_{k-1}, x_k)\omega}$
$(q_1', q_2') = (q_1', q_2')\tau_\nu^0 = (q_1'\tau_\nu', q_2'\tau_\nu^{2^{q_1'}}) \Rightarrow q_1'\tau_\nu^{2^{q_1'}} = q_2'$
$(q_1', q_2'') = (q_1', q_2')\tau_\omega^0 = (q_1'\tau_\omega', q'\tau_\omega^{2^{q_1'}}) \Rightarrow q_1'\tau_\omega^{2^{q_1'}} = q_2''$
$(q_1', q_2') = (q_1', q_2'')\tau_\nu^0 = (q_1''\tau_\nu', q_2''\tau_\nu^{2^{q_1''}}) \Rightarrow q_1''\tau_\nu^{2^{q_1''}} = q_2'$
$(q_1', q_2'') = (q_1', q_2'')\tau_\omega^0 = (q_1''\tau_\omega', q_2''\tau_\omega^{2^{q_1''}}) \Rightarrow q_1''\tau_\omega^{2^{q_1''}} = q_2''$

Dwz de restricties van τ_λ^2, $\tau_\nu^{2^{q_1'}}$ en $\tau_\omega^{2^{q_1'}}$ tot $\{q_2', q_2''\}$ vormen een semigroep isomorf met $(S_2, \ )$, dus
$$(S_2, \ ) \mid (S_{A_2}, \ ).$$

9.1.7. $\aleph_0=\aleph_1 \textcircled{\omega} \aleph_2 \geq \aleph$.
$(S_1, \ ) \mid (S_A, \ ) \Rightarrow (S_1, \ ) \mid (S_{A_1}, \ ) \vee (S_1, \ ) \mid (S_{A_2}, \ )$

bewijs: Evenals in het bewijs van 9.1.6. vinden we mbv. 9.1.3. een ondersemigroep van $(S_{A_0}, \ )$ die isomorf is met $(S_1, \ )$, nl. $(\{\tau_{\lambda^0}, \tau_{\nu^0}\}, \ )$.
$\exists_{(q_1,q_2)\in Q_0}\left[(q_1, q_2)\tau_\nu^0 = (q_1', q_2') \neq (q_1, q_2)\right] \Rightarrow (q_1', q_2')\tau_\nu^0 = (q_1, q_2)\tau_\nu^0\tau_\nu^0 = (q_1, q_2)\tau_\nu^0 = (q_1', q_2')$
Twee gevallen:
1. $q_1' \neq q_1 \Rightarrow \tau_\lambda' \neq \tau_\nu' \Rightarrow (S_1, \ )$ is een ondersemigroep van $(S_{A_1}, \ )$.
2. $q_1' = q_1 \Rightarrow q_2' \neq q_2$
$(q_1', q_2') = (q_1, q_2)\tau_\nu^0 = (q_1\tau_\nu', q_2\tau_\nu^{2^{q_1}})$ dwz. $q_2\tau_\nu^{2^{q_1}} = q_2'$.
De restrictie van τ_λ^2 en $\tau_\nu^{2^{q_1}}$ tot q_2, q_2' vormt een semigroep isomorf met $(S_1, \ )$ en dus
$$(S_1, \ ) \mid (S_{A_2}, \ ).$$

9.1.8. Een toestandsautomaat $\mathcal{A}$ is onontleedbaar slals $(S_{\mathcal{A}},)$ een enkelvoudige groep of $\mathcal{A}$ een resettoestandsautomaat met twee toestanden is.

bewijs: Dat $\mathcal{A}$ ontleedbaar is, als $(S_{\mathcal{A}},)$ niet aan de genoemde voorwaarden voldoet, volgt uit de hoofdstelling.
Voldoet $\mathcal{A}$ wel aan de voorwaarden, dan volgt uit 9.1.2., 9.1.3., 9.1.6. en 9.1.7. de stelling.

ECB-525

AFSTUDEER-OPDRACHT GROEP ECB

Onderwerp: Semigroepen en Sequentiële Machines

Toelichting:

De structuur van een sequentiële machine is nauw verwant aan de structuur van de semigroep, welke de machine beschrijft.
Decompositie, uitgevoerd via semigroepen, is waarschijnlijk gemakkelijker te hanteren en te automatiseren dan via partities.
Gevraagd wordt hier een studie van te maken en een eenvoudige decompositie te programmeren.

Naam: R.H.J.M.Otten

Adres: Wenzelweg 26

Woonplaats: Eindhoven

Inschrijfnr.: 3757

Mentor: ir. Ekas

IN TE VULLEN DOOR MENTOR

Datum aanvang: 1 februari 1971

Datum beeindiging: 10/11/71

Datum inlevering afstudeerverslag: ± 25/11/71

Advieswaardering mentor: Zeer goede presentatie, onderzoek en een
verslag.
Na ± 1 week nog 2 dgds in toegevoegd aan
definitief verslag. (25/11)

Cijfer: 9½ 9½

Bonnr.: 13502 10

Aantal bladen:

Adressen.

1. Sectiebibliotheek:	de secretaresse.
2. Componenten:	mentor.
3. Documentatie:	hr. Q.L.M.Laarhoven.
4. Meetapparaten (advies):	hr. Q.L.M.Laarhoven.
5. Meetapparaten (uitleen):	hr. Q.L.M.Laarhoven.
6. Gereedschappen:	hr. Q.L.M.Laarhoven.

Bij het lenen van boeken, dokumentatie, apparatuur etc. dient het eerste blad, voor het registreren van het bovengenoemde, mede gebracht te worden.

Geleende boeken en dokumentatie dienen gedurende de werktijden (8.30-17.45) aanwezig te zijn.

Meetapparatuur mag niet geleend worden zonder de bijbehorende beschrijving mede in ontvangst te nemen. De inhoud hiervan wordt vóór het ingebruik nemen van de apparatuur bekend verondersteld.
Defecten dienen onverwijld te worden gemeld. In geval van schade wordt beoordeeld of de gebruiker aansprakelijk gesteld dient te worden.

Een standaardset gereedschap kan worden verstrekt.

De in de groep gebruikelijke montage- en meettechnieken dient U te volgen. Inlichtingen hierover verkrijgt U van Uw mentor.

Na afloop van de werkzaamheden, dient U zorg te dragen dat op de adressen 1 t/m 6 akkoord parafen worden verstrekt als teken dat U de betreffende apparaten, boeken etc. hebt ingeleverd.

Algemeen.

Wanneer men de keuze heeft bepaald van de afstudeerrichting, en deze keuze is gevallen op de groep ECB, is het goed enkele punten te overwegen.
In de eerste plaats is het van belang dat U goede contacten onderhoudt met Uw mede-afstuderenden. Deze contacten moeten naast de persoonlijke ook technisch zijn, d.w.z. het is van belang dat U met Uw medestudenten ervaringen uitwisselt waardoor Uw inzicht wordt verbreed en verscherpt.
Daarnaast wordt van U verwacht dat U studenten die stages lopen behulpzaam bent door het geven van inlichtingen.

Persoonlijk stel ik diskussies bijzonder op prijs wanneer ik bij U kom kijken naar de vorderingen van het werk. Een goed en levendig contact met de aan U toegewezen wetenschappelijke medewerker is vanzelfsprekend van het hoogste belang.

Over de vorderingen van Uw werkzaamheden kunt U de staf regelmatig voorlichten tijdens bijeenkomsten van de staf en alle studenten die in de groep ECB afstuderen en stages verrichten. Deze voordrachten vind ik zo belangrijk dat zij verplicht zijn gesteld voor alle studenten zoals boven vermeld. U dient deze voordrachten eenmaal per vier weken te houden.

Teneinde een goed inzicht te hebben van de bestede tijd wordt U verzocht 's morgens en 's avonds gelijktijdig met het overige personeel van de groep Uw werk aan te vangen en te beëindigen. Dit heeft bovendien als voordeel dat U een regelmatiger en meer efficiënte dagindeling krijgt.

Het afstudeerwerk wordt afgesloten met een zakelijk verslag dat het eigendom is van de T.H. Indien de tijd dit toelaat kan het verslag door personeel van de T.H. worden verzorgd. Indien de tijd dit niet toelaat moet U het verlag duidelijk leesbaar en reproduceerbaar schrijven of typen.

prof. ir. A.Heetman.

Eindige automaten en semigroepen

Om inzicht te krijgen in de wijze waarop automaten ontleed kunnen worden in eenvoudigere machines, associëren we met elke machine een semigroep. We kunnen dan bewijzen dat een machine altijd ontleed kan worden in eenvoudigere machines, tenzij ze een flip-flop is, of een semigroep heeft die een enkelvoudige groep is. Omgekeerd geldt ook dat elke ontleedbare machine opgebouwd kan worden uit flip-flops en enkelvoudige-groep-automaten, terwijl er een nauwkeurig omschreven relatie bestaat tussen de enkelvoudige groepen en de semigroep van de oorspronkelijke machine.

Dit verslag is bedoeld als een inleiding tot de grondbegrippen van de semigroep-theoretische benadering van automaten. Bewijzen worden niet gegeven en wiskundige begrippen worden meestal intuitief ingevoerd.

1. Semigroepen.

Als men twee verzamelingen heeft, A en B, die beide niet leeg zijn, dan kan men een nieuwe verzameling definiëren, nl die van alle geordende paren (a,b) waarbij $a \in A$ en $b \in B$. We noemen deze verzameling het carthesisch product en geven hem aan met $A \times B$:

$$(a,b) \in A \times B \iff ((a \in A) \wedge (b \in B))$$

We kunnen voor de tweede verzameling dezelfde als de eerste nemen. Een afbeelding $m: A \times A \to A$ noemen we een binaire bewerking. Denk b.v. A als de verzameling der gehele getallen en de bewerking als vermenigvuldigen.

We gaan nu een ~~ab~~ aantal algebraïsche structuren definiëren

Een semigroep is een verzameling S en een bewerking $m: S \times S \to S$ met de eigenschappen: $S \neq \emptyset$

$$\forall_{a \in S} \forall_{b \in S} \forall_{c \in S} [m(m(a,b),c) = m(a,m(b,c))]$$

(associativiteit).

Een semigroep (S,m) heet een monoïde als

$$\exists_{e \in S} \forall_{a \in S} [m(a,e) = m(e,a) = a]$$

(e heet de eenheid van het monoïde)

Een monoïde (G,m) heet een groep als

$$\forall_{a \in G} \exists_{a^{-1} \in G} [m(a,a^{-1}) = m(a^{-1},a) = e]$$

(a^{-1} heet de inverse van a)

(S',m) is een ondersemigroep van de semigroep (S,m) als

$$S' \subseteq S$$

$$\forall_{a \in S'} \forall_{b \in S'} [m(a,b) \in S']$$

Ter verduidelijking geven we een voorbeeld:

Zij X een alfabet van eindig veel symbolen. Met de elementen van X kunnen we symbooltrijen maken die we woorden noemen. De verzameling van alle woorden, opgebouwd uit eindig veel symbolen, geven we aan met X^∞:

$$\sigma_1 \sigma_2 \ldots \sigma_n \in X^\infty \iff \sigma_i \in X$$

Bij semigroepen hebben we behalve een verzameling, ook een bewerking. We definiëren daarom de bewerking "concatenatie":

$$m(\sigma_1 \sigma_2 \ldots \sigma_n, \sigma_1' \sigma_2' \ldots \sigma_m') = \sigma_1 \sigma_2 \ldots \sigma_n \sigma_1' \sigma_2' \ldots \sigma_m'$$
waarbij $\sigma_1 \sigma_2 \ldots \sigma_n \in X^\infty$
$\sigma_1' \sigma_2' \ldots \sigma_m' \in X^\infty$

Deze bewerking is associatief en gesloten over X^∞, dus (X^∞, m) is een semigroep. Er is echter geen element e, de eenheid, in X^∞.
We voegen daarom aan de verzameling X^∞ de lege symboolrij toe en geven deze aan met Λ. Λ bevat dus geen enkel symbool.
De nieuwe verzameling geven we aan met X^*:

$$X^* = X^\infty \cup \{\Lambda\}$$

Daar nu geldt: $\forall_{\bar{x} \in X^*} \; [m(\Lambda, \bar{x}) = \bar{x} = m(\bar{x}, \Lambda)]$

is (X^*, m) een monoïde. We noemen het het door X gegenereerde vrije monoïde.

Opmerking: We schrijven voortaan voor (S, m) S en voor $m(a, b)$ ab

2. Eindige automaten

Een eindig automaat is $M = (X, Y, Q, \delta, \lambda)$, waarin
- X: een eindig inputalfabet
- Y: een eindig outputalfabet
- Q: een eindige verzameling toestanden
- $\delta: Q \times X \to Q$ overgangsfunctie
- $\lambda: Q \times X \to Y$ responsiefunctie.

We definiëren nu op de volgende manier voortzettingen van δ en λ:

$$\delta^*: Q \times X^* \to Q \quad \text{met} \quad \delta^*(q, \Lambda) = q$$
$$\delta^*(q, \bar{x} x_i) = \delta(\delta^*(q, \bar{x}), x_i)$$

$$\lambda^*: Q \times X^* \to Y \quad \text{met} \quad \lambda^*(q; \bar{x} x_i) = \lambda(\delta^*(q, \bar{x}), x_i)$$

We zien dat $\lambda(q, \Lambda)$ niet gedefinieerd is

Alleen machines waarmee we vanuit de begintoestand elke andere toestand kunnen bereiken door de inputwaarden geschikt te kiezen komen van nu af aan nog ter sprake!

3. Het verband tussen een machine en zijn semigroep.

Gewoonlijk kan men een machine ~~met~~ $M(f)$ met een overgangstabel beschrijven. Aan de hand van het volgende eenvoudige voorbeeld, wil ik laten zien hoe men tot de semigroep van $M(f)$ kan komen:

	0	1
q_0	q_1	q_2
q_1	q_2	q_1
q_2	q_2	q_2

Overgangstabel van $M(f)$

Als elementen van de semigroep van $M(f)$ beschouw ik de klassen van inputrijen die op de toestand van $M(f)$ het zelfde effect hebben. Als $\bar{x}$ en $\bar{y}$ in dezelfde klasse zitten, en $M(f)$ is een willekeurige toestand q, dan heeft de inputrij $\bar{x}$ als ook de inputrij $\bar{y}$ tot gevolg dat $M(f)$ in de toestand q' komt:

	Λ	0	1	00	01	10	11
q_0	q_0	q_1	q_2	q_2	q_1	q_2	q_2
q_1	q_1	q_2	q_1	q_2	q_2	q_2	q_1
q_2	q_2	q_2	q_2	q_2	q_2	q_2	q_2

De kolom onder "0" is identiek aan die onder "01", zoook die onder "1" en "11" en die onder "00" en "10".
"0" en "01" zitten daarom in de zelfde klasse : $s_1 = [0] = [01]$
"1" en "11" ook : $s_2 = [1] = [11]$
"00" en "10" idem : $s_3 = [00] = [10]$

Inputrijen van meer symbolen als 2 hoef ik niet meer na te gaan maar de kolommen onder symboolrijen die met "00" of "10" beginnen als nieuwe toestand steeds q_2 leveren en alle andere inputrijen gevormd kunnen worden uit de reeds gegeven kolommen.

De klasse van Λ geven we aan met s_0

	s_0	s_1	s_2	s_3
q_0	q_0	q_1	q_2	q_2
q_1	q_1	q_2	q_1	q_2
q_2	q_2	q_2	q_2	q_2

	s_0	s_1	s_2	s_3
s_0	s_0	s_1	s_2	s_3
s_1	s_1	s_3	s_1	s_3
s_2	s_2	s_3	s_2	s_3
s_3	s_3	s_3	s_3	s_3

"Cayley"-tabel van de semigroep van $M(f)$

De laatste tabel komt als volgt tot stand:

Ik heb een inputrij uit de klasse s_i en de laat deze volgen door een inputrij uit de klasse s_j. De klasse waartoe ~~de~~ de totale inputrij $s_i s_j$ hoort plaats ik dan in de rij van s_i en in de kolom van s_j

De verzameling $S_f = \{s_0, s_1, s_2, s_3\}$ en de bewerking concatenatie vormen een semigroep, want concatenatie is associatief en gesloten over S_f (er komen in de tabel immers alleen maar elementen van S_f voor).

In ons voorbeeld is de semigroep groter als de overgangstabel. Hoe groot kan zo'n semigroep worden? Het antwoord is zonder meer verontrustend: Als het aantal toestanden van $M(f)$ n is dan:

$$n \leq |S| \leq n^n$$

Beide grenzen bereikbaar!

Hierboven hebben we, uitgaande van de overgangstabel van $M(f)$, de semigroep S_f afgeleid. ~~Uiteraard willen~~ Natuurlijk willen we ook bij een gegeven semigroep S een machine $M(S)$ vinden die S als zijn semigroep heeft. Dit is overigens zeer eenvoudig. Dit ziet men direkt in als men de Cayley-tabel van S als overgangstabel ziet. Voor de rijen staat de toestands s_i waarin de machine zich bevindt. We geven de input s_j. De nieuwe toestand wordt $s_i . s_j$ D.w.z:

$$M(S) = (S, S, S, \cdot, \cdot).$$

Meestal zijn we echter speciaal in het transduktiegedrag van een machine geïnteresseerd, zodat de gegeven $M(S)$ niet geheel bevredigd. We modificeren het antwoord daarom maar een klein beetje:

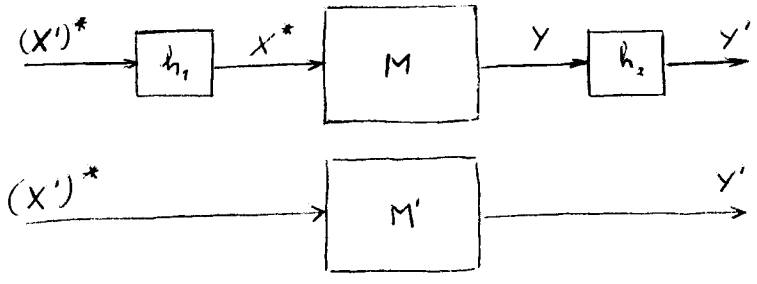
$$M(S, i) = (S, Y, S, \cdot, i)$$

waarbij $\quad i : S \to Y$

4. Deelbaarheid.

Belangrijk is nu, te ontdekken wat het verband is tussen $M(f)$ en $M(S_f, i_f)$. Hierbij speelt het (machinetheoretische) begrip "simuleren" een rol:

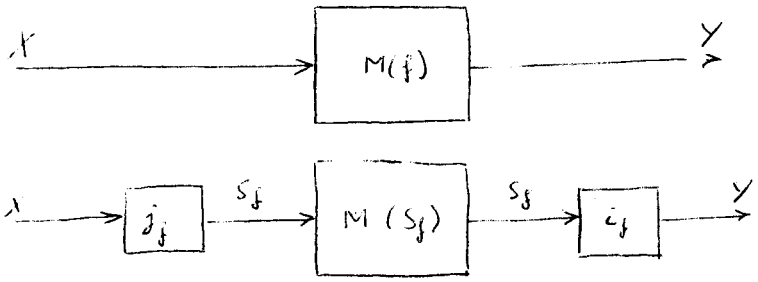
De machine M simuleert een machine M' als er een geschikte codeer- en decodeernetwerk aan M toegevoegd kan worden, zodat het transduktiegedrag van M' bereikt wordt.



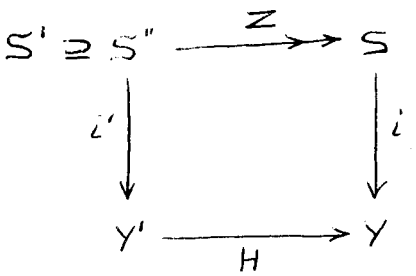
Als M M' simuleert, dan zeggen we "M' deelt M": $\quad M' \,|\, M$

Twee machines heten zwak equivalent als $M' \,|\, M$ en $M \,|\, M'$

We kunnen nu bewijzen dat $M(f)$ en $M(S_f, i_f)$ zwak equivalent zijn.



Voor semigroepen willen we nu een soortgelijk concept "delen" hebben. We introduceren dit begrip aan de hand van het volgende diagram:



Z is hierbij een afbeelding van een ondersemigroep S'' van S' op S waarbij geldt

$$\forall_{s \in S''} \; \forall_{s' \in S'} \; [Z(s.s') = Z(s).Z(s')]$$

(d.w.z. Z is een homomorfisme)

We zeggen nu

$$S \mid S' \iff S' \supseteq S'' \xrightarrow{Z} S$$

en

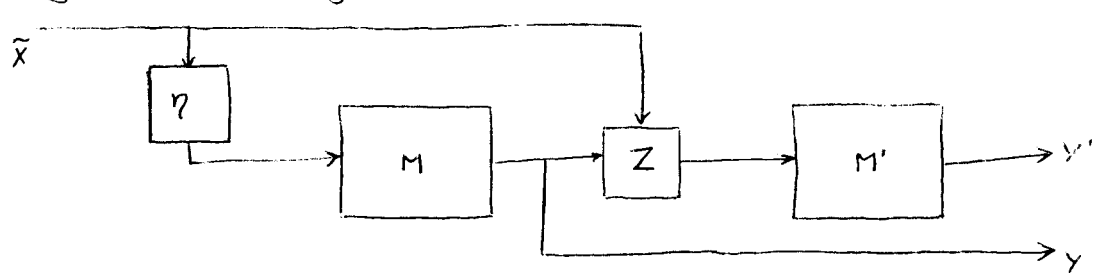
$$(S, i) \mid (S', i') \iff \{\forall_{s \in S''} \; [\, i(Z(s)) = H(i'(s)) \,]\} \wedge S \mid S'$$

Hiermee hebben we bereikt wat we willen, want men kan bewijzen dat

$$M(g) \mid M(f) \iff (S_g, i_g) \mid (S_f, i_f)$$

5. Ontleding van automaten

Een cascade is een schakeling met twee machines die als volgt onderling verbonden zijn



η en Z zijn hier combinatorische netwerken.

We noemen een machine M s-irreducibel als voor elke cascade van twee machines M_1 en M_2, die M simuleert, geldt: $M \mid M(S_1)$ of $M \mid M(S_2)$

Elke machine $M(f)$ kan gesimuleerd worden door cascades van flip-flops en machines, waarvan de semigroepen enkelvoudige groepen zijn die de semigroep S_f delen.

Bovenstaande stelling (in 1962 bewezen door Krohn en Rhodes) kan beschouwd worden als de hoofdstelling van deze theorie

Tot slot bekijken we de componenten waaruit elke machine opgebouwd kan worden:

Allereerst de flip-flop met de volgende overgangstabel:

F	e x_0 x_1	
q_0	q_0 q_0 q_1	set-reset-flip-flop
q_1	q_1 q_0 q_1	

Zijn semigroep is dan:

U_3	1	r_0	r_1	
1	1	r_0	r_1	
r_0	r_0	r_0	r_1	semigroep U_3
r_1	r_1	r_0	r_1	

Deze semigroep heeft nog 3 ondersemigroepen: $U_2 = \{r_0, r_1\}$
$U_1 = \{1, r_0\} \simeq \{1, r_1\}$
$U_0 = \{1\}$.

Hiermee formuleren we dan de volgende stelling.

Machines met als semigroep een enkelvoudige groep of een semigroep isomorf met U_3, U_2, U_1 of U_0 zijn s-irreducibel

6. Enkelvoudige groepen.

Het zou te ver gaan hier de groepentheorie tot aan de enkelvoudige groepen hier te behandelen. De klassifikatie van groepen is nog onopgelost en een van de meest aktuele onderwerpen in dit vakgebied. We geven daarom slechts een overzicht met wat commentaar om twee vragen te beantwoorden:

- Voor welke orden (dwz aantal elementen van een groep) bestaan er enkelvoudige groepen?
- Als de orde bepaald is, is er dan slechts één enkelvoudige groep van die orde?

Om met vraag 1 te beginnen. Er bestaan enkvoudige groepen

- voor orden die een priemgetal. Deze zijn dus cyclisch (dus ook commutatief) en de bijbehorende machines zijn teller
- voor orden $\frac{1}{2}n!$ met $n > 4$, nl. de alternerende groepen.

60, 360, 2520, ---

- projectieve unimodulaire groepen: de eerste orden zijn 168, 504, 660, 1092
- nog enkele "sporadische" orden alle groter als 7920.

Het antwoord op de tweede vraag is ontkennend; er zijn enkelvoudige groepen van gelijke orde en niet isomorf. De kleinste orde is 20160

$$|A_8| = |PSL(3,4)| = 20160 \quad \text{en} \quad A_8 \not\cong PSL(3,4)$$

7. Groepmachines

Stel we hebben een eindige groep $(G, *)$ dus G is een eindige verzameling. $(H, *)$ heet dan een ondergroep van $(G, *)$ als

$$H \subseteq G \quad \text{èn} \quad (H, *) \text{ is een groep}$$

Kiezen we nu uit G een element g en vermenigvuldigen we elke element h van H hiermee (links) dan krijgen we een verzameling met evenveel elementen als H. We geven haar aan met $g * H$ en noemen haar een linkernevenklasse van H

$$g * H = \{ g * h \mid h \in H \}$$

H is zelf ook een nevenklasse, immers $e * H = H$.

De verzameling van linkernevenklassen vormt een partitie op G. Dit betekent, dat

$$\bigcup_{g \in G} [g * H] = G$$

èn $\quad g_1 * H \cap g_2 * H \neq \emptyset \Rightarrow g_1 * H = g_2 * H$

Dit heeft tot gevolg dat een bepaald element c eenduidig een nevenklasse vertegenwoordigen kan. Zo'n c heet een representant van die klasse. Voor elke linkernevenklasse kan je zo'n representant c_i aanwijzen. De groep G is dan te schrijven als:

$$G = \bigcup_{i=1}^{|G|/|H|} [c_i * H]$$

Voor de rechternevenklasse

$$H * g = \{ h * g \mid h \in H \}$$

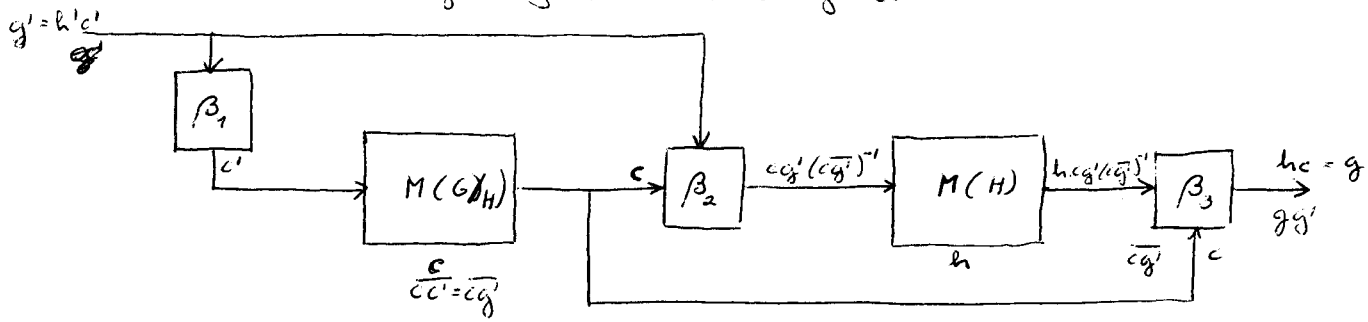
kunnen we een analoog verhaal houden.
Natuurlijk hoeft niet te gelden dat $g * H = H * g$, maar als hier voor elke $g \in G$ aan voldaan is, dan noemen we H een normale ondergroep van G.
In zo'n geval kunnen we op de verzameling van nevenklassen een bewerking definiëren waarvoor geldt

$$(g_1 * H) * (g_2 * H) = (g_1 * g_2) * H$$

De aldus gedefinieerde structuur is een groep en we noemen haar een faktorgroep aangeduid met $(G/H, *)$

Beschouwen we nu een machine die als semigroep de groep G heeft. Als $M(G)$ dan in toestand g is en hij krijgt ~~toestand~~ input g' dan gaat hij over in gg'

We onderzoeken nu het gedrag van de volgende cascade



We noteren de representant c van de nevenklasse Hg met $\bar{g}$

Stel nu $g = hc$

De hele cascade is in toestand g
De machine $M(G/H)$ is in toestand $c = \bar{g}$
De machine $M(H)$ is in toestand h
Dus

$$\beta_3 = (h, c) = hc = g.$$

We geven nu een input $g' = h'c'$ met $c' = \bar{g'}$
dan geven we $M(G/H)$ de input $\bar{g'} = c'$, waardoor deze machine overgaat in $\overline{cc'} = \overline{cg'}$

Het combinatorisch netwerk β_2 verzorgt de input voor $M(H)$. β_2 krijgt c en g' aangeboden en geeft aan $M(H)$ $cg'(c\bar{g'})^{-1}$

$$\beta_2(c, g') = cg'(c\bar{g'})^{-1}$$

Het is gemakkelijk na te gaan dat de output van β_2 een element van H is. Onder deze input gaat $M(H)$ van toestand h over in toestand $h.cg'(c\bar{g'})^{-1}$
β_3 krijgt nu aangeboden $h.cg'(c\bar{g'})^{-1}$ en $\overline{cg'}$. De output van de cascade is dus

$$\beta_3(h.cg'(c\bar{g'})^{-1}, \overline{cg'}) = hcg'(c\bar{g'})^{-1}c\bar{g'} = hcg' = gg'$$

De cascade simuleert de groepmachine $M(G)$ dus volledig

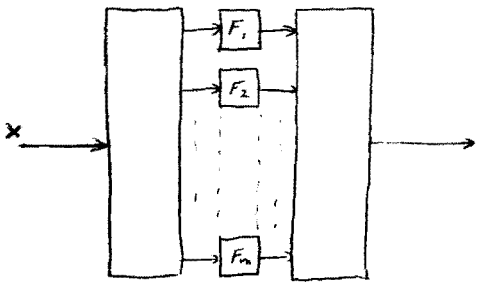
$M(G/H)$ en $M(H)$ zijn weer groepmachines en als ze dus echte normale ondergroepen hebben, dan zouden we ze ook op deze manier in een cascade kunnen ontleden. Op deze manier krijgt men een beeld van samenstellen van faktorgroepen die enkelvoudig zijn. Immers een enkelvoudige groep is per definitie een groep die geen echte normale ondergroep heeft

8. IR-machines

Een IR-machine is een machine waarvoor geldt dat bij elke input $x \in X$ de machine òf in de toestand blijft waarin hij was òf onafhankelijk van de toestand waarin hij zich bevindt overgaat in een toestand q die dan dus slechts van x afhangt

Een eenvoudig voorbeeld van een IR machine is de set-reset-flip-flop F met semigroep U_3 uit §5. Met deze machines in cascade kan elke IR-machine gemaakt worden.

Stel bv de IR-machine heeft n toestanden. Kies dan het kleinste gehele getal m waarvoor $n \leq 2^m$



(m.b.v. die m F-machines zijn 2^m toestanden te coderen).

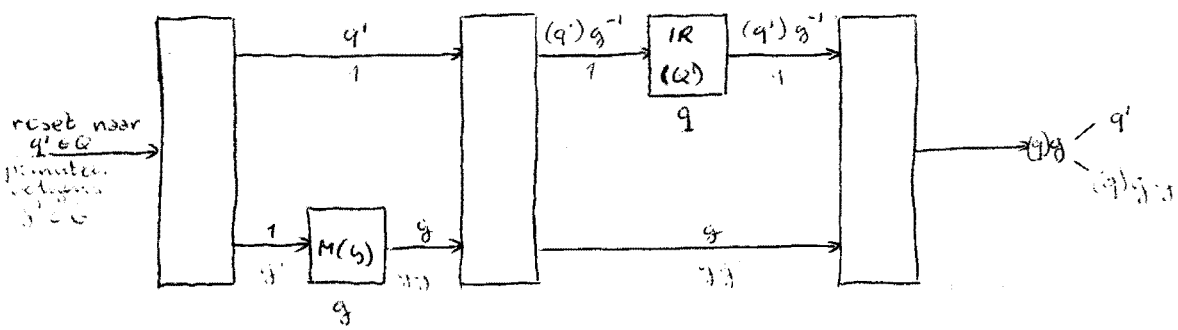
9. PR-machines

Een PR-machine is een machine waarvoor elke input $x \in X$ òf een toestandspermutatie òf een constante afbeelding op een q die alleen van x afhangt, veroorzaakt

dus òf $\delta(\cdot, x)$ is 1-1 òf $\delta(\cdot, x) = q(x)$ voor $x \in X$

Wanneer we even alleen naar de permutatie-inputs kijken dan genereren deze een groep G. Dit heet de groep van de PR-machine (dit is niet de semigroep van de PR-machine!)

De volgende cascade laat zien dat elke PR-machine M met zijn groepmachine $M(G)$ en een IR-machine met alle toestanden van M gemaakt kan worden



$(q)g$ is het effect van de permutatie g op q