Voorwoord

Ter afsluiting van mijn studie Informatica aan de Rijksuniversiteit Leiden, heb ik gekozen voor een afstudeerproject op het gebied van de Theoretische informatica, een specialisatie van de afstudeerrichting Fundamentele informatica. De inhoud van dit project is de trace-theorie; een theorie die verband houdt met formele talen en concurrente systemen. In deze afstudeerscriptie zal een beslisbaarheidsprobleem met betrekking tot trace-talen worden behandeld.

Dank gaat uit naar mijn afstudeerdocent dr. Hendrik J. Hoogeboom. Door zijn goede begeleiding en overzichtelijke uitleg kan ik terug zien op een aangename en vooral leerzame periode.

Rijnsburg, juli 1994.
Gerrit N. Bouknecht.

Inhoudsopgave

Voorwoord **i**

1 Inleiding **1**

1.1 De trace-theorie 1
1.2 Het probleem 2
1.3 Een kort overzicht 2

2 Basisbegrippen **5**

2.1 Relaties 5
2.2 Grafen 5
2.3 Monoïden 6
2.4 Het vrije en directe product 8
2.5 De commutatieve afbeelding 9
2.6 Reguliere expressies en rationele verzamelingen 10
2.7 Automaten 11
2.8 Semilineaire verzamelingen 12

3 De doorsnede en het product **13**

3.1 Bipartiete automaten 13
3.2 De doorsnede en het vrije product 15
3.3 De doorsnede en het directe product 16

4 De doorsnede over trace-monoïden **19**

4.1 Een klasse van trace-monoïden waarvoor het doorsnedeprobleem onbeslisbaar is 19
4.2 Een klasse van trace-monoïden waarvoor het doorsnedeprobleem beslisbaar is 21

5 Conclusie **23**

A Een alternatief bewijs **25**

Literatuuroverzicht **29**

Referenties **31**

Hoofdstuk 1

Inleiding

1.1 De trace-theorie

In [16] introduceerde Mazurkiewicz de trace-theorie als een wiskundig hulpmiddel voor het beschrijven van het gedrag van concurrente systemen. De verzameling acties van het concurrente systeem wordt hierbij gerepresenteerd door middel van een alfabet. Acties kunnen onafhankelijk van elkaar zijn; de volgorde waarin ze worden uitgevoerd is dan niet van belang. Dit komt tot uitdrukking in een onafhankelijkheidsrelatie over het alfabet. Letters uit het alfabet zijn onafhankelijk van elkaar wanneer de corresponderende acties onafhankelijk zijn. In de trace-theorie wordt het gedrag beschreven door middel van sequentiële observaties. Zo'n sequentiële observatie bestaat uit een woord over het alfabet. Meerdere sequentiële observaties van een en hetzelfde proces kunnen echter van elkaar verschillen. Deze observaties zijn dan wel equivalent aan elkaar in die zin dat de ene observatie uit de andere verkregen kan worden door het verwisselen van naast elkaar gelegen onafhankelijke letters. De verzameling van alle equivalente observaties, de equivalentieklasse, van een gegeven sequentiële observatie, noemen we een trace. Een trace geeft ons dus volledige informatie over het gedrag van het geobserveerd proces.

Neem als voorbeeld de sequentiële observatie aabcab, en laat alleen a en b onafhankelijk van elkaar zijn, dan is de trace behorende bij aabcab gelijk aan de verzameling $\{\mathrm{aabcab}, \mathrm{abacab}, \mathrm{baacab}, \mathrm{aabcba}, \mathrm{abacba}, \mathrm{baacba}\}$.

Een verzameling van traces noemen we een trace-taal. Een trace-taal is dus een beschrijving, al of niet volledig, van het gedrag van een concurrent systeem. De trace-theorie is een theorie over trace-talen, waarbij soortgelijke (beslisbaarheids)problemen worden behandeld als bij de 'klassieke' formele talen, maar dan modulo equivalentie. In het verdere verloop van deze scriptie behandelen we een trace-taal dan ook als een formele taal over woorden en hun equivalentieklassen, zonder daarbij aandacht te besteden aan de achterliggende concurrente systemen.

Zoals we later zullen zien, zijn trace-talen op te vatten als deelverzamelingen van vrije partieel commutatieve monoïden. Op dit gebied werd al eerder onderzoek gedaan door Cartier en Foata in [7], waar gekeken wordt naar combinatorische problemen die ontstaan bij het rangschikken van woorden.

Zie het artikel van Aalbersberg en Rozenberg in [2] voor een overzicht van de trace-theorie.

1.2 Het probleem

Met betrekking tot concurrente systemen kunnen we verschillende beslisbaarheidsproblemen bekijken. Zo kunnen we ons afvragen of twee concurrente systemen hetzelfde gedrag vertonen. Wanneer K en L de trace-talen zijn die het gedrag van deze systemen beschrijven, dan komt dit overeen met de vraag of $K = L$. Ook kan het interessant zijn om te onderzoeken of het ene systeem deel uitmaakt van het andere systeem, wat leidt tot de vraag of $K \subseteq L$.

In deze scriptie houden we ons bezig met een ander beslisbaarheidsprobleem, namelijk het doorsnedeprobleem: gegeven twee trace-talen K en L, is $K \cap L$ leeg? In termen van concurrente systemen is dit de vraag of twee systemen een of meerdere processen gemeenschappelijk hebben. We bekijken alleen het geval waarbij K en L rationele trace-talen zijn, dit zijn trace-talen die we door middel van reguliere expressies of eindige automaten kunnen definiëren, zie Hoofdstuk 2. Het zal blijken dat de oplosbaarheid van dit probleem afhangt van de onafhankelijkheidsrelatie, en niet, zoals we misschien verwachten, altijd oplosbaar is.

Het doorsnedeprobleem voor dit soort talen is al behandeld in [1] door Aalbersberg en Hoogeboom. Stelling 4.5, de stelling waar het in deze scriptie eigenlijk omgaat, wordt daarin bewezen, zie Theorem 2.8 in [1]. De bewijsvoering verschilt echter. Hier benaderen we het probleem door middel van monoïden, een begrip dat in het volgende hoofdstuk nader zal worden toegelicht. Door op een abstracte manier te werken met monoïden zullen de stellingen in Hoofdstuk 3 algemener van aard zijn, en daarmee in principe breder toepasbaar. Verder maken we gebruik van bipartiete automaten, zie Hoofdstuk 3. De reden voor deze benadering is te vinden in [20]. Sakarovitch behandelt daar een ander beslisbaarheidsprobleem met betrekking tot tracetalen en maakt daarbij gebruik van monoïden en bipartiete automaten. In zijn conclusie deelt hij mee dat het bewijs van Theorem 2.8 in [1] op soortgelijke wijze gedaan lijkt te kunnen worden.

1.3 Een kort overzicht

In Hoofdstuk 2 worden een aantal basisbegrippen behandeld. Naast begrippen als transitief bos, monoïde, rationele deelverzameling, vrije en directe product, worden de commutatieve afbeelding en de semilineaire verzamelingen gedefinieerd. Vervolgens wordt in Hoofdstuk 3 gekeken naar de doorsnede toegepast op deelverzamelingen van monoïden die zijn ontstaan door gebruik van het vrije en directe product. Voor de monoïden waarnaar wordt gekeken, zal aangetoond worden dat de commutatieve afbeelding van de doorsnede van rationele deelverzamelingen semilineair is. Het vrije en directe product zal vervolgens in Hoofdstuk 4 gebruikt worden om de zogenaamde trace-monoïden te bepalen waarvoor het doorsnedeprobleem beslisbaar is. Het zal blijken dat die trace-monoïden een transitief bos als onafhankelijkheidsalfabet hebben. In Hoofdstuk 4 zal ook gekeken worden naar trace-monoïden waarvoor het doorsnedeprobleem niet beslisbaar is. Na dit hoofdstuk volgt de conclusie.

In Appendix A wordt een alternatief bewijs besproken van een van de stellingen uit Hoofdstuk 3.

Aan het eind van deze scriptie bevindt zich een kort literatuuroverzicht. Hierin worden een aantal andere beslisbaarheidsproblemen besproken die betrekking hebben op trace-talen.

Hoofdstuk 2

Basisbegrippen

2.1 Relaties

Laat A een verzameling zijn. Een deelverzameling $R \subseteq A \times A$ heet een *relatie* op A. We schrijven vaak aRb in plaats van $(a,b) \in R$. Relatie R heet *reflexief* als $(a,a) \in R$ voor alle $a \in A$, *irreflexief* als $(a,a) \notin R$ voor alle $a \in A$, *symmetrisch* als $(a,b) \in R$ impliceert dat $(b,a) \in R$, en *transitief* als $(a,b) \in R$, $(b,c) \in R$ impliceert dat $(a,c) \in R$.

Een reflexieve, symmetrische, en transitieve relatie noemen we een *equivalentierelatie*. Laat $R \in A \times A$ een equivalentierelatie zijn. De *equivalentieklasse* van $a \in A$, genoteerd $[a]_R$, is de verzameling $\{x \in A \mid (a,x) \in R\}$.

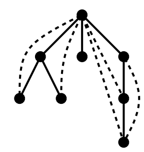
2.2 Grafen

Een *ongerichte graaf* G is een 2-tupel (V,E), met V een verzameling knopen, en $E \subseteq V \times V$ een verzameling ongerichte takken, dit wil zeggen als $(v,w) \in E$, dan $(w,v) \in E$. We spreken in het vervolg gewoon over een *graaf* wanneer we een ongerichte graaf bedoelen. Verder noteren we het paar $(v,w),(w,v)$, met $v \neq w$, als $\{v,w\}$. Een *pad* in G is een rijtje knopen $(v_0, v_1, \ldots, v_n)$, met $n \geq 1$, zodanig dat, voor alle $0 \leq i < n$, $(v_i, v_{i+1}) \in E$. Een pad $(v_0, v_1, \ldots, v_n)$ in G, met $n \geq 3$, heet een *cykel* wanneer, voor alle $0 \leq i < j < n$, $v_i \neq v_j$, en $v_0 = v_n$. De graaf G is *samenhangend* wanneer voor iedere $v, w \in V$ geldt dat er een pad is van v naar w. Een graaf (V', E') is een *(geïnduceerde) subgraaf* van graaf (V,E) wanneer geldt dat $V' \subseteq V$, en $E' = E \cap (V' \times V')$. We noemen twee grafen (V_1, E_1) en (V_2, E_2) *disjunct* wanneer V_1 en V_2 disjunct zijn.

We definiëren nu een tweetal operaties op disjuncte grafen.

Definitie 2.1 *Laat (V_1, E_1), (V_2, E_2) disjuncte grafen zijn.*

1. *De* vereniging $(V_1, E_1) \cup (V_2, E_2)$ *is de graaf* $(V_1 \cup V_2, E_1 \cup E_2)$.



Figuur 2.1: Een transitieve boom.

2. *De* som $(V_1, E_1) + (V_2, E_2)$ *is de graaf* $(V_1 \cup V_2, E_1 \cup E_2 \cup (V_1 \times V_2) \cup (V_2 \times V_1))$.

Een *boom* is een samenhangende graaf zonder cykels. Een *bos* is een vereniging van bomen. Een *georiënteerde boom* is een boom met een speciale knoop die we wortel noemen. Een *georiënteerd bos* is een vereniging van georiënteerde bomen. We spreken in het vervolg gewoon over een boom en een bos wanneer we een georiënteerde boom respectievelijk een georiënteerd bos bedoelen. Wanneer w de wortel is van boom T en $(v_0, v_1, \ldots, v_n)$ een pad in T, met $w = v_0$, $n \geq 1$, en voor alle $0 \leq i < j \leq n$, $v_i \neq v_j$, dan noemen we v_j een afstammeling van v_i wanneer $i < j$, en spreken over een directe afstammeling wanneer $i = j - 1$. Een blad is een knoop zonder afstammelingen.

Een speciaal soort grafen zijn de transitieve bomen en bossen.

Definitie 2.2 *Een* transitieve boom *is een graaf die het resultaat is van een boom T waaraan de takken $\{v, w\}$, met w een afstammeling van v in T, zijn toegevoegd. Een* transitief bos *is een vereniging van transitieve bomen.*

Een voorbeeld van een transitieve boom is gegeven in Figuur 2.1. De wortel van de boom is bovenaan getekend, en de toegevoegde takken zijn gestippeld.

Het is eenvoudig in te zien dat transitieve bossen precies die grafen zijn die recursief als volgt zijn gedefinieerd. Een graaf met een enkele knoop is een transitief bos. Zij T_1, T_2 transitieve bossen. De graaf $T_1 \cup T_2$ is een transitief bos. De graaf $T_1 + T_2$ is een transitief bos wanneer T_1 of T_2 uit een enkele knoop bestaat.

2.3 Monoïden

De definitie van het begrip monoïde luidt als volgt.

Definitie 2.3 *Een* monoïde *is een 3-tupel $(M, \cdot_M, 1_M)$, met M een verzameling, $\cdot_M$ een associatieve binaire operatie op M, en $1_M \in M$ een eenheidselement. Verzameling M is gesloten onder $\cdot_M$.*

Wanneer dit geen verwarring oplevert noteren we monoïde $(M, \cdot_M, 1_M)$ kortweg als M, operatie $\cdot_M$ als $\cdot$, en eenheidselement 1_M als 1. We staan toe dat in expressies de $\cdot$ wordt weggelaten, dus $m_1 \cdot m_2$ wordt ook geschreven als $m_1 m_2$. Verder schrijven we $M^\bullet$ voor $M \setminus 1_M$. Een monoïde M heeft *eenheidsdelers* wanneer er elementen $m_1, m_2 \in M^\bullet$ zijn zodanig dat $m_1 \cdot m_2 = 1_M$.

Zij $K, L \subseteq M$. We definiëren $K \cdot_M L = \{k \cdot_M l \mid k \in K, l \in L\}$, $K^0 = \{1_M\}$, $K^i = K \cdot_M K^{i-1}$, voor $i > 0$, $K^+ = \bigcup_{i=1}^{\infty} K^i$, en $K^* = K^+ \cup \{1_M\}$. Monoïde M is *(eindig) voortgebracht* door K wanneer geldt dat $M = K^*$ (en K is eindig).

Een alfabet is een eindige verzameling. Laat Σ een alfabet zijn. De *vrije monoïde* Σ^* is de welbekende verzameling van eindige rijtjes van elementen uit Σ, met de concatenatie als monoïde operator, en het lege rijtje als eenheidselement.

Een congruentie over een monoïde M is een equivalentierelatie $\equiv$ waarvoor geldt, voor $m_1, m_2 \in M$, dat $m_1 \equiv m_1'$, $m_2 \equiv m_2'$ impliceert dat $m_1 m_2 \equiv m_1' m_2'$.

Zij $\equiv$ een congruentie op monoïde M. De *quotiëntmonoïde* $M/\equiv$ is de monoïde waarvan de elementen gevormd worden door de equivalentieklassen van $\equiv$, en waarbij de operatie gedefinieerd is door, voor $m_1, m_2 \in M$, $[m_1]_\equiv \cdot_{M/\equiv} [m_2]_\equiv = [m_1 \cdot_M m_2]_\equiv$.

Een *onafhankelijkheidsalfabet* is een 2-tupel $C = (\Sigma, I)$, met Σ een alfabet, en $I \subseteq \Sigma \times \Sigma$ een irreflexieve, symmetrische relatie. We noemen I de *onafhankelijkheidsrelatie*. Een onafhankelijkheidsalfabet is op te vatten als graaf. De terminologie uit paragraaf 2.2 kunnen we dus ook gebruiken voor een onafhankelijkheidsalfabet. We definiëren nu de relatie $\equiv_C \subseteq \Sigma^* \times \Sigma^*$ als de kleinste congruentie waarvoor geldt, voor alle $(a, b) \in I$, $ab \equiv_C ba$.

We definiëren de vrije partieel commutatieve monoïden en de vrije commutatieve monoïden.

Definitie 2.4 *Laat $C = (\Sigma, I)$ een onafhankelijkheidsalfabet zijn. De* vrije partieel commutatieve monoïde *of* trace-monoïde *behorende bij (Σ, I), genoteerd $\mathrm{M}(\Sigma, I)$, is de quotiëntmonoïde $\Sigma^*/\equiv_C$. Elementen uit $\mathrm{M}(\Sigma, I)$ noemen we* traces, *en deelverzamelingen van $\mathrm{M}(\Sigma, I)$ noemen we* trace-talen.

We zeggen dat monoïde $\mathrm{M}(\Sigma', I')$ een *submonoïde* van monoïde $\mathrm{M}(\Sigma, I)$ is, wanneer (Σ', I') een subgraaf van (Σ, I) is.

Definitie 2.5 *Laat Σ een alfabet zijn. De* vrije commutatieve monoïde *voortgebracht door Σ, genoteerd $\Sigma^\oplus$, is de vrije partieel commutatieve monoïde $\mathrm{M}(\Sigma, I)$, met $I = \{(a, b) \in \Sigma \times \Sigma \mid a \neq b\}$.*

Een element van de vrije commutatieve monoïde $\Sigma^\oplus$ kan opgevat worden als een afbeelding in $\mathbf{N}^\Sigma$, alleen het aantal voorkomens van de voortbrengers is namelijk van belang. We kunnen een vrije commutatieve monoïde $\Sigma^\oplus$ daarom ook opvatten als een monoïde $(M, +_M, 0_M)$, met $M = \mathbf{N}^\Sigma$, en $+_M$ de optelling van elementen uit M gedefinieerd door, voor $\psi_1, \psi_2 \in M$, $\psi_1 + \psi_2 = \psi$, zodanig dat $\psi \in M$, en $\psi(a) = \psi_1(a) + \psi_2(a)$, voor alle $a \in \Sigma$.

We definiëren over een monoïde $M \times C$ de M-doorsnede.

Definitie 2.6 *Laat M, C monoïden zijn. Met de M-*doorsnede *van twee verzamelingen $K, L \subseteq M \times C$ bedoelen we de verzameling $\{(x, y, z) \mid (x, y) \in K$ en $(x, z) \in L\}$. De M-doorsnede noteren we als $\overset{M}{\cap}$.*

Het resultaat van de M-doorsnede over $M \times C$ is dus een deelverzameling van monoïde $M \times C \times C$.

Laat M, N monoïden zijn. Een *homomorfisme* van M naar N is een functie $\varphi : M \to N$ zodanig dat $\varphi(1_M) = 1_N$, en $\varphi(m_1 \cdot_M m_2) = \varphi(m_1) \cdot_N \varphi(m_2)$, voor alle $m_1, m_2 \in M$. Een *isomorfisme* van M naar N is een bijectief homomorfisme $\varphi : M \to N$. We noemen twee monoïden M en N *isomorf*, genoteerd $M \simeq N$, wanneer er een isomorfisme bestaat van M naar N.

2.4 Het vrije en directe product

Het *vrije product* van monoïden M en N, genoteerd $M * N$, met M en N disjunct, is de monoïde bestaande uit rijtjes van elementen alternerend uit $M^\bullet$ en $N^\bullet$. De monoïde operatie $*_{M*N}$ toegepast op rijtjes $(x_1, \ldots, x_m), (y_1, \ldots, y_n) \in M * N$ is als volgt recursief gedefinieerd. Het vrije product $(x_1, \ldots, x_m) *_{M*N} (y_1, \ldots, y_n)$ is gelijk aan $(x_1, \ldots, x_m, y_1, \ldots, y_n)$, als x_m en y_1 niet uit dezelfde monoïde komen, gelijk aan $(x_1, \ldots, x_m \cdot_M y_1, \ldots, y_n)$, als $x_m, y_1 \in M$ en $x_m \cdot_M y_1 \neq 1_M$, gelijk aan $(x_1, \ldots, x_m \cdot_N y_1, \ldots, y_n)$, als $x_m, y_1 \in N$ en $x_m \cdot_N y_1 \neq 1_N$, en gelijk aan $(x_1, \ldots, x_{m-1}) *_{M*N} (y_2, \ldots, y_n)$, als $x_m, y_1 \in M$ en $x_m \cdot_M y_1 = 1_M$, of als $x_m, y_1 \in N$ en $x_m \cdot_N y_1 = 1_N$.

Het *directe product* van monoïden M en N, genoteerd $M \times N$, is de monoïde bestaande uit elementen (m, n), met $m \in M$, en $n \in N$. De monoïde operatie $\cdot_{M \times N}$ toegepast op elementen $(m_1, n_1), (m_2, n_2) \in M \times N$ is als volgt gedefinieerd: $(m_1, n_1) \cdot_{M \times N} (m_2, n_2) = (m_1 \cdot_M m_2, n_1 \cdot_N n_2)$.

Voor grafen hebben we de operaties vereniging en som gedefinieerd. In de volgende stelling wordt het verband aangegeven tussen deze operaties toegepast op onafhankelijkheidsalfabets en het vrije en directe product toegepast op bijbehorende trace-monoïden. Het bewijs laten we achterwege.

Stelling 2.7 *Laat $\mathrm{M}(\Sigma_1, I_1)$, $\mathrm{M}(\Sigma_2, I_2)$ trace-monoïden zijn, met (Σ_1, I_1), (Σ_2, I_2) disjunct. Er geldt:*

1. $\mathrm{M}((\Sigma_1, I_1) \cup (\Sigma_2, I_2)) \simeq \mathrm{M}(\Sigma_1, I_1) * \mathrm{M}(\Sigma_2, I_2)$.
2. $\mathrm{M}((\Sigma_1, I_1) + (\Sigma_2, I_2)) \simeq \mathrm{M}(\Sigma_1, I_1) \times \mathrm{M}(\Sigma_2, I_2)$.

In paragraaf 2.2 is het verband aangegeven tussen grafen opgebouwd door middel van de operaties vereniging en som en de transitieve bossen. We kunnen nu hetzelfde doen voor monoïden opgebouwd door middel van het vrije en directe product. Trace monoïden waarvan het onafhankelijkheidsalfabet gevormd wordt door een transitief bos, zijn precies die trace-monoïden die isomorf zijn met de monoïden die recursief als volgt zijn gedefinieerd. Een trace-monoïde voortgebracht door een enkele letter heeft een transitief bos als onafhankelijkheidsalfabet. Laat M, N monoïden zijn isomorf met trace-monoïden waarvan het onafhankelijkheidsalfabet gevormd wordt door een transitief bos. De monoïde $M * N$ is isomorf met een trace-monoïde waarvan het onafhankelijkheidsalfabet gevormd wordt door een transitief bos. De monoïde $M \times N$ is isomorf met een trace-monoïde waarvan het onafhankelijkheidsalfabet gevormd wordt door een transitief bos wanneer M of N voortgebracht wordt door een enkele letter.

2.5 De commutatieve afbeelding

De commutatieve afbeelding gebruiken we wanneer we bij elementen uit een monoïde alleen geïnteresseerd zijn in het aantal voorkomens van de voortbrengers, en niet in hun volgorde.

Definitie 2.8 *Laat M een monoïde zijn voortgebracht door Σ. Het homomorfisme $\psi_\Sigma : M \to \Sigma^\oplus$ gedefinieerd door, voor $a \in \Sigma$, $\psi_\Sigma(a) = a$, noemen we de* commutatieve afbeelding *over M.*

Wanneer we de vrije commutatieve monoïde $\Sigma^\oplus$ opvatten als de monoïde $\mathbf{N}^\Sigma$, dan kunnen we bovenstaand homomorfisme ook definiëren door, voor $a \in \Sigma$, $\psi_\Sigma(a) = \psi$, zodanig dat $\psi \in \mathbf{N}^\Sigma$, $\psi(a) = 1$, en $\psi(b) = 0$, voor alle $b \in \Sigma \setminus \{a\}$.

De commutatieve afbeelding bestaat voor trace-monoïden. Er zijn echter monoïden waarvoor deze afbeelding niet bestaat. Neem bijvoorbeeld een monoïde M met eenheidsdelers m_1, m_2, dus $m_1 m_2 = 1$. Een element $m \in M$ kunnen we nu schrijven als $m m_1 m_2$, of als $m m_1 m_1 m_2 m_2$, en zo verder. De commutatieve afbeelding bestaat dus niet voor deze monoïde.

In het algemeen geldt dat de commutatieve afbeelding bestaat voor een monoïde M voortgebracht door Σ dan en slechts dan als er een homomorfisme $\varphi_2 : M \to \Sigma^\oplus$ bestaat zodanig dat $\psi_\Sigma = \varphi_2 \circ \varphi_1$, met ψ_Σ de commutatieve afbeelding over de vrije monoïde Σ^*, en $\varphi_1 : \Sigma^* \to M$ het homomorfisme gedefinieerd door, voor $a \in \Sigma$, $\varphi_1(a) = a$. We zeggen dan dat de commutatieve afbeelding over de vrije monoïde Σ^* factorizeert over monoïde M. Zie Figuur 2.2.

We bekijken nu monoïden van de vorm $M \times C \times C$. Laat M voortgebracht worden door Σ, en C door Δ. De voortbrengers van $M \times C \times C$ zijn dan

$$\begin{tikzcd}
\Sigma^* \arrow[rr, "\psi_\Sigma"] \arrow[dr, "\varphi_1"'] & & \Sigma^\oplus \\
& M \arrow[ur, "\varphi_2"'] &
\end{tikzcd}$$

Figuur 2.2: De commutatieve afbeelding.

van de vorm $(a, 1, 1)$, $(1, b, 1)$, $(1, 1, b)$, met $a \in \Sigma$, en $b \in \Delta$. Echter, de vrije commutatieve monoïde over deze voortbrengers is isomorf met de monoïde $\Sigma^\oplus \times \Delta^\oplus \times \Delta^\oplus$. Voor de commutatieve afbeelding kunnen we in dit geval daarom gebruik maken van de volgende definitie.

Definitie 2.9 *Laat M een monoïde zijn voortgebracht door Σ, en C een monoïde voortgebracht door Δ. De* commutatieve afbeelding *over $M \times C \times C$ is de functie $\psi_{\Sigma,\Delta} : M \times C \times C \to \Sigma^\oplus \times \Delta^\oplus \times \Delta^\oplus$ gedefinieerd door, voor $m \in M$ en $c_1, c_2 \in C$, $\psi_{\Sigma,\Delta}(m, c_1, c_2) = (\psi_\Sigma(m), \psi_\Delta(c_1), \psi_\Delta(c_2))$.*

2.6 Reguliere expressies en rationele verzamelingen

We maken gebruik van reguliere expressies om verzamelingen of talen te definiëren.

Definitie 2.10 *Laat M een monoïde zijn voortgebracht door Σ. Een* reguliere expressie *over M wordt als volgt recursief gedefinieerd.*

1. *$\emptyset$ is een reguliere expressie en geeft de lege verzameling aan.*
2. *1 is een reguliere expressie en geeft de verzameling $\{1_M\}$.*
3. *voor alle $a \in \Sigma$, is a een reguliere expressie en geeft de verzameling $\{a\}$.*
4. *Als α en β reguliere expressies zijn die respectievelijk de verzamelingen A en B definiëren, dan zijn $(\alpha + \beta)$, $(\alpha\beta)$, en (α^*) reguliere expressies die respectievelijk de verzamelingen $A \cup B$, $A \cdot_M B$, en A^* geven.*

Aan de hand van reguliere expressies definiëren we nu de klasse van rationele deelverzamelingen.

Definitie 2.11 *Laat M een monoïde zijn. De klasse van* rationele *deelverzamelingen van M, genoteerd $\mathrm{Rat}(M)$, is de klasse van verzamelingen die gedefinieerd worden door de reguliere expressies over M.*

Het is duidelijk dat deze klasse gesloten is onder de operaties $\cup$, $\cdot_M$, en *. Deze klasse is echter niet voor elke monoïde M gesloten onder doorsnede en verschil. Het volgende voorbeeld laat dit zien voor de doorsnede. Omdat de doorsnede verkregen kan worden door middel van vereniging en verschil volgt hieruit, als M eindig voortgebracht is, het niet gesloten zijn onder verschil. Laat $M = \mathrm{M}(\{\mathrm{a},\mathrm{b}\},\emptyset) \times \mathrm{M}(\{\mathrm{c}\},\emptyset)$ een monoïde zijn, en $K, L \in \mathrm{Rat}(M)$, met $K = (\mathrm{a},\mathrm{c})^*(\mathrm{b},1)^*$, $L = (\mathrm{a},1)^*(\mathrm{b},\mathrm{c})^*$. We krijgen: $K \cap L = \{(\mathrm{a}^n\mathrm{b}^n, \mathrm{c}^n) \mid n \geq 0\}$. Hieruit volgt dat de doorsnede van K en L niet rationeel is. Immers, de verzameling $\{\mathrm{a}^n\mathrm{b}^n \mid n \geq 0\}$ is niet rationeel, en de klasse van rationele deelverzamelingen is gesloten onder projectie.

2.7 Automaten

Naast de reguliere expressies maken we ook gebruik van automaten om verzamelingen of talen te definiëren (danwel te herkennen).

Definitie 2.12 *Laat M een monoïde zijn. Een* automaat *over M is een 5-tupel $\mathcal{A} = (Q, M, E, I, T)$ met*

Q	*een eindige verzameling toestanden,*
$E : Q \times Q \to 2^M$	*een verzameling gelabelde takken,*
$I \subseteq Q$	*een verzameling begintoestanden,*
$T \subseteq Q$	*een verzameling eindtoestanden.*

Een tak is gelabeld met een deelverzameling van M. Deze verzameling hoeft niet eindig te zijn. De reden hiervoor is te vinden in Hoofdstuk 3, waar we de bipartiete automaten introduceren. Een tak gelabeld met een verzameling A is op te vatten als een verzameling van takken, ieder gelabeld met een element uit A. We zeggen dat er een pad is van q naar q' in $\mathcal{A}$ gelabeld m, ook genoteerd als $q \xrightarrow{m} q'$, wanneer er een rij $q_0, q_1, \ldots, q_n$, met $n \geq 1$, $q = q_0$, en $q' = q_n$, bestaat zodanig dat, voor alle $0 \leq i < n$, $E(q_i, q_{i+1}) = K_{i+1}$, en $m \in K_1 \cdot K_2 \cdot \ldots \cdot K_n$. De verzameling die door de automaat wordt herkend is de verzameling $\mathcal{L}(\mathcal{A}) = \{m \in M \mid$ er is een pad van $q \in I$ naar $q' \in T$ in $\mathcal{A}$ gelabeld $m\}$.

Met de *automaat over een monoïde* bedoelen we hier niet de in de literatuur bekende *monoïde automaat*, zie bijvoorbeeld [4]. Bij de monoïde automaat hebben we namelijk nog de eis: als $m_1 \in E(q_0, q_1)$, $m_2 \in E(q_1, q_2)$, en $m_1 m_2 = m_2 m_1$, dan is er een q_1' zodanig dat $m_2 \in E(q_0, q_1')$, en $m_1 \in E(q_1', q_2)$.

We maken ook gebruik van automaten waarvan de takken gelabeld zijn met eindige verzamelingen.

Definitie 2.13 *Laat M een monoïde zijn. De automaat $\mathcal{A} = (Q, M, E, I, T)$ heet* eindig *als, voor alle $q_1, q_2 \in Q$, $E(q_1, q_2)$ een eindige verzameling is.*

Zoals bekend is de klasse van verzamelingen die gedefinieerd worden door middel van eindige automaten gelijk aan de klasse van verzamelingen die gedefinieerd worden door middel van reguliere expressies (stelling van Kleene). Een verzameling die gedefinieerd wordt door een eindige automaat is dus rationeel.

2.8 Semilineaire verzamelingen

We maken gebruik van bepaalde deelverzamelingen van de vrije commutatieve monoïden, namelijk de semilineaire verzamelingen. Een handige eigenschap van deze verzamelingen is dat zij gesloten zijn onder vereniging, doorsnede en verschil. We definiëren semilineaire verzamelingen in termen van lineaire verzamelingen.

Definitie 2.14 *Een deelverzameling van een vrije commutatieve monoïde* $\Sigma^\oplus$ *heet* lineair *wanneer deze geschreven kan worden als* $\{x\}\{y_1\}^* \cdots \{y_n\}^*$, *met* $n \geq 0$, *en* $x, y_1, \ldots, y_n \in \Sigma^\oplus$.

De lineaire verzamelingen zijn gesloten onder de operaties $\cdot$, en *. Immers, $\{x\}\{y_1\}^* \cdots \{y_n\}^* \cdot \{x'\}\{y'_1\}^* \cdots \{y'_m\}^* = \{xx'\}\{y_0\}^* \cdots \{y_n\}^*\{y'_1\}^* \cdots \{y'_m\}^*$, en $(\{x\}\{y_1\}^* \cdots \{y_n\}^*)^* = \{1\}\{x\}^*\{y_1\}^* \cdots \{y_n\}^*$.

Definitie 2.15 *Een eindige vereniging van lineaire verzamelingen heet* semilineair.

De semilineaire verzamelingen worden dus verkregen door de operaties $\cup$, $\cdot$, en * op eindige deelverzamelingen van $\Sigma^\oplus$ toe te passen. Zij zijn tevens gesloten onder deze operaties. Voor de operatie $\cup$ is dit duidelijk. Voor de operatie $\cdot$ volgt dit uit het feit dat de operatie $\cdot$ toegepast op semilineaire verzamelingen gelijk is aan de vereniging van lineaire verzamelingen waarop de operatie $\cdot$ is toegepast. Voor de operatie * volgt dit uit de vergelijking $(A \cup B)^* = A^*B^*$, met A en B (semi)lineaire verzamelingen. We mogen nu de conclusie trekken dat de klasse van semilineaire verzamelingen gelijk is aan $\mathrm{Rat}(\Sigma^\oplus)$.

Ginsburg heeft in [13] het volgende bewezen.

Stelling 2.16 *De semilineaire verzamelingen zijn gesloten onder doorsnede en verschil.*

In het geval dat Σ, Δ disjunct zijn geldt dat $(\Sigma \cup \Delta)^\oplus \simeq \Sigma^\oplus \times \Delta^\oplus$. We kunnen daarom spreken over semilineaire verzamelingen in $\Sigma^\oplus \times \Delta^\oplus$. Verder staan we toe te spreken over semilineaire verzamelingen in $\Sigma^\oplus \times \Delta^\oplus \times \Delta^\oplus$, waarbij we dus twee copieën van Δ gebruiken.

Wanneer we in het vervolg spreken over een verzameling die semilineair is, dan bedoelen we daarmee dat de commutatieve afbeelding van die verzameling semilineair is.

Hoofdstuk 3

De doorsnede en het product

In dit hoofdstuk wordt voor bepaalde monoïden bewezen dat de doorsnede van rationele deelverzamelingen semilineair is. Stelling 3.6 handelt hierbij over monoïden die opgebouwd worden door middel van het vrije product, en Stelling 3.9 over monoïden die opgebouwd worden door middel van het directe product. Voor Stelling 3.6 hebben we het begrip bipartiete automaat nodig.

3.1 Bipartiete automaten

De definitie van een bipartiete automaat, zoals wij die gebruiken, luidt als volgt.

Definitie 3.1 *Laat M, N, C monoïden zijn. De automaat $\mathcal{A} = (Q, (M*N) \times C, E, I, T)$ heet* bipartiet *als $Q = P \cup R$, met P en R disjunct, en $E = E_P \cup E_R$, met $E_P : P \times R \to 2^{M \times C}$, $E_R : R \times P \to 2^{N \times C}$.*

We noteren $\mathcal{A} = (P \cup R, (M * N) \times C, E_P \cup E_R, I_P \cup I_R, T_P \cup T_R)$, met $I_P = I \cap P$, $I_R = I \cap R$, $T_P = T \cap P$, $T_R = T \cap R$.

Het zal duidelijk zijn waarom we de benaming bipartiet gebruiken. Er zijn alleen takken van $p \in P$ naar $r \in R$, en andersom, maar geen takken tussen elementen van P of R onderling. Deze definitie wijkt echter af van de definitie die door Sakarovitch in [20] gegeven wordt. De bipartiete automaat die daar wordt gedefinieerd is een automaat over monoïde $M * N$, met, voor $p \in P$, $r \in R$, $E_P(p, r) \subseteq M$, en $E_R(r, p) \subseteq N$. Dus de takken die gelabeld zijn met elementen van M wijzen alleen de ene kant op, en de takken die gelabeld zijn met elementen van N de andere kant. In ons geval echter kunnen takken die gelabeld zijn met $\{1\} \times C$ zowel de ene kant als de andere kant op wijzen. Waarom we hier de bipartiete automaat definiëren over $(M * N) \times C$, en niet over $M * N$, zal blijken in de volgende paragrafen.

In Stelling 3.6 maken we gebruik van bipartiete automaten om een eigenschap te bewijzen van de $(M * N)$-doorsnede over een monoïde $(M * N) \times C$. Hiertoe definiëren we de (M, N)-productconstructie.

Definitie 3.2 *Laat* $\mathcal{B}_1 = (P_1 \cup R_1, (M*N) \times C, E_{P_1} \cup E_{R_1}, I_{P_1} \cup I_{R_1}, T_{P_1} \cup T_{R_1})$, $\mathcal{B}_2 = (P_2 \cup R_2, (M*N) \times C, E_{P_2} \cup E_{R_2}, I_{P_2} \cup I_{R_2}, T_{P_2} \cup T_{R_2})$ *bipartiete automaten zijn. Het* (M, N)-product *van* $\mathcal{B}_1$ *en* $\mathcal{B}_2$ *is de bipartiete automaat* $\mathcal{B} = (P \cup R, (M*N) \times C \times C, E_P \cup E_R, I_P \cup I_R, T_P \cup T_R)$, *met* $P = P_1 \times P_2$, $R = R_1 \times R_2$, $I_P = I_{P_1} \times I_{P_2}$, $I_R = I_{R_1} \times I_{R_2}$, $T_P = T_{P_1} \times T_{P_2}$, $T_R = T_{R_1} \times T_{R_2}$, *en voor alle* $(p_1, p_2) \in P$, $(q_1, q_2) \in R$, $E_P((p_1, p_2), (q_1, q_2)) = E_{P_1}(p_1, q_1) \overset{M}{\cap} E_{P_2}(p_2, q_2)$, $E_R((q_1, q_2), (p_1, p_2)) = E_{R_1}(q_1, p_1) \overset{N}{\cap} E_{R_2}(q_2, p_2)$.

Voor het product geldt dus dat de takken de ene kant op gelabeld zijn met elementen van $M \times C \times C$, en de andere kant op met elementen van $N \times C \times C$.

Het toepassen van het (M, N)-product op willekeurige bipartiete automaten levert niet zondermeer de $(M*N)$-doorsnede op. We definiëren daarom de volgende eigenschap.

Definitie 3.3 *Een bipartiete automaat* $(P \cup R, (M*N) \times C, E_P \cup E_R, I_P \cup I_R, T_P \cup T_R)$ *voldoet aan* Eigenschap 1 *wanneer voor iedere* $p \in P$, $r \in R$ *geldt:*

1. *als er een pad bestaat van* p *naar* r *gelabeld* $m \in M \times C$, *dan* $m \in E_P(p, r)$,
2. *als er een pad bestaat van* r *naar* p *gelabeld* $n \in N \times C$, *dan* $n \in E_R(r, p)$.

Het volgende lemma laat nu zien dat de $(M*N)$-doorsnede over verzamelingen die gedefinieerd zijn door middel van bipartiete automaten die voldoen aan Eigenschap 1, gegeven wordt door de bipartiete automaat die ontstaat door het (M, N)-product toe te passen op deze automaten.

Lemma 3.4 *Laat* $\mathcal{B}_1$, $\mathcal{B}_2$ *bipartiete automaten over monoïde* $(M*N) \times C$ *zijn die voldoen aan Eigenschap 1, en* $\mathcal{B}$ *de bipartiete automaat die onstaat door het* (M, N)-*product toe te passen op* $\mathcal{B}_1$ *en* $\mathcal{B}_2$. *Er geldt nu dat* $\mathcal{L}(\mathcal{B}) = \mathcal{L}(\mathcal{B}_1) \overset{M*N}{\cap} \mathcal{L}(\mathcal{B}_2)$.

Bewijs: Stel $(x, c, c') \in \mathcal{L}(\mathcal{B})$, er is dus een pad (van een begin- naar eindknoop) in $\mathcal{B}$ gelabeld (x, c, c'). Het is duidelijk dat er dan een pad in $\mathcal{B}_1$ moet zijn gelabeld (x, c) en een pad in $\mathcal{B}_2$ gelabeld (x, c'). Hieruit volgt dat $(x, c, c') \in \mathcal{L}(\mathcal{B}_1) \overset{M*N}{\cap} \mathcal{L}(\mathcal{B}_2)$.

Stel $(x, c, c') \in \mathcal{L}(\mathcal{B}_1) \overset{M*N}{\cap} \mathcal{L}(\mathcal{B}_2)$. Omdat $\mathcal{B}_1$ en $\mathcal{B}_2$ aan Eigenschap 1 voldoen is er een pad in $\mathcal{B}_1$ waarvan de achtereenvolgende takken gelabeld zijn met $(x_1, c_1), (x_2, c_2), \ldots, (x_n, c_n)$, en een pad in $\mathcal{B}_2$ waarvan de achtereenvolgende takken gelabeld zijn met $(x_1, c'_1), (x_2, c'_2), \ldots, (x_n, c'_n)$, zodanig dat $x = x_1 x_2 \cdots x_n$, $c = c_1 c_2 \cdots c_n$, $c' = c'_1 c'_2 \cdots c'_n$, met x_i alternerend uit M en N, en $c_i, c'_i \in C$. Dit betekent dat er een pad in $\mathcal{B}$ bestaat waarvan de takken achtereenvolgens gelabeld zijn met $(x_1, c_1, c'_1), (x_2, c_2, c'_2), \ldots, (x_n, c_n, c'_n)$. Hieruit volgt dat $(x, c, c') \in \mathcal{L}(\mathcal{B})$. $\square$

De automaten $\mathcal{B}_1$ en $\mathcal{B}_2$ moeten aan Eigenschap 1 voldoen. Is dit niet het geval, dan kunnen we niet garanderen dat bijvoorbeeld het pad van $\mathcal{B}_1$ uit bovenstaand bewijs bestaat uit achtereenvolgende takken die gelabeld zijn met $(x_1, c_1), (x_2, c_2), \ldots, (x_n, c_n)$. Het label (x_i, c_i) kan dan ook afkomstig zijn van een pad bestaande uit meerdere takken, bijvoorbeeld $(x_i', c_i'), (1, c), (x_i'', c_i'')$, waardoor het bewijs niet meer correct zou zijn.

3.2 De doorsnede en het vrije product

We kunnen voor een rationele deelverzameling van monoïde $(M * N) \times C$ een bipartiete automaat construeren die aan bepaalde eisen voldoet, mits M en N aan een bepaalde eis voldoen.

Lemma 3.5 *Laat M, N, C monoïden zijn, met de eis dat M en N geen eenheidsdelers hebben. Dan geldt voor iedere rationele deelverzameling van $(M * N) \times C$ dat hij het resultaat is van een* bipartiete automaat *over $(M * N) \times C$ die aan* Eigenschap 1 *voldoet en waarvan de takken gelabeld zijn met* rationele deelverzamelingen *van $M \times C$ en $N \times C$.*

Bewijs: Zij $K \in \mathrm{Rat}((M * N) \times C)$ en $\mathcal{A} = (Q, (M * N) \times C, E, I, T)$ de eindige automaat die K als resultaat heeft, dus $K = \mathcal{L}(\mathcal{A})$. We mogen er vanuit gaan dat de takken gelabeld zijn met elementen uit $(M \times C) \cup (N \times C)$. Immers een tak die gelabeld is met $(x_1 x_2 \cdots x_n, c)$, met x_i alternerend uit $M^\bullet$ en $N^\bullet$, kan vervangen worden door een pad waarvan de takken achtereenvolgens gelabeld zijn met $(x_1, 1), (x_2, 1), \ldots, (x_n, 1), (1, c)$.

We construeren nu een bipartiete automaat $\mathcal{B} = (P \cup R, (M * N) \times C, E_P \cup E_R, I_P \cup I_R, T_P \cup T_R)$, met $P = Q \times \{\mathrm{p}\}$, $R = Q \times \{\mathrm{r}\}$, $I_P = I \times \{\mathrm{p}\}$, $I_R = I \times \{\mathrm{r}\}$, $T_P = T \times \{\mathrm{p}\}$, $T_R = T \times \{\mathrm{r}\}$, $E_P((q_1, \mathrm{p}), (q_2, \mathrm{r})) = \{m \mid$ er is een pad van q_1 naar q_2 in $\mathcal{A}$ gelabeld m over takken die gelabeld zijn met elementen uit $M \times C\}$, en $E_R((q_2, \mathrm{r}), (q_1, \mathrm{p})) = \{n \mid$ er is een pad van q_2 naar q_1 in $\mathcal{A}$ gelabeld n over takken die gelabeld zijn met elementen uit $N \times C\}$.

Er geldt $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$. Immers, wanneer $x \in \mathcal{L}(\mathcal{A})$, dan is er een pad $q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \ldots \xrightarrow{x_n} q_n$, met $q_0 \in I$ en $q_n \in T$, in $\mathcal{A}$, waarbij x_i alternerend uit $M \times C$ en $N \times C$, en $x = x_1 x_2 \cdots x_n$. Maar dit betekent dat er ook een pad $(q_0, y_0) \xrightarrow{x_1} (q_1, y_1) \xrightarrow{x_2} \ldots \xrightarrow{x_n} (q_n, y_n)$ in $\mathcal{B}$ bestaat, waarbij y_i alternerend uit $\{\mathrm{p}\}$ en $\{\mathrm{r}\}$. Aangezien $(q_0, y_0) \in I_P \cup I_R$ en $(q_n, y_n) \in T_P \cup T_R$ volgt hieruit dat $x \in \mathcal{L}(\mathcal{B})$. Andersom is op dezelfde manier te bewijzen dat voor een willekeurige $x \in \mathcal{L}(\mathcal{B})$ er een pad te vinden is in $\mathcal{A}$ die gelabeld is met x, waaruit dan volgt dat $x \in \mathcal{L}(\mathcal{A})$.

Het is ook duidelijk dat de takken van $\mathcal{B}$ gelabeld zijn met rationele deelverzamelingen van $M \times C$ respectievelijk $N \times C$. De verzamelingen zijn namelijk het resultaat van eindige automaat $\mathcal{A}$ waaruit de takken die gelabeld zijn met elementen uit $N^\bullet \times C$ respectievelijk $M^\bullet \times C$ zijn verwijderd en waarin de begin- en eindtoestanden zijn gewijzigd.

We moeten nu alleen nog laten zien dat $\mathcal{B}$ aan Eigenschap 1 voldoet. Zij $(q_1, \mathrm{p}) \in P$ en $(q_2, \mathrm{r}) \in R$. Wanneer er een pad is van (q_1, p) naar (q_2, r) in $\mathcal{B}$ gelabeld $m \in M \times C$, dan is er ook een pad van q_1 naar q_2 in $\mathcal{A}$ gelabeld m. Omdat N geen eenheidsdelers heeft geldt voor het pad in $\mathcal{A}$ dat deze bestaat uit takken die gelabeld zijn met elementen uit $M \times C$. Maar dit betekent dat $m \in E_P((q_1, \mathrm{p}), (q_2, \mathrm{r}))$. Evenzo voor een pad van (q_2, r) naar (q_1, p) in $\mathcal{B}$ gelabeld $n \in N \times C$, krijgen we dat $n \in E_P((q_2, \mathrm{r}), (q_1, \mathrm{p}))$. $\Box$

Met behulp van Lemma 3.4 en 3.5 kunnen we nu aantonen dat monoïden die opgebouwd worden door middel van het vrije product aan een cruciale eigenschap voldoen.

Stelling 3.6 *Laat M, N, C monoïden zijn, waarvoor de commutatieve afbeeldingen bestaan. Als respectievelijk de M-doorsnede over* $\mathrm{Rat}(M \times C)$ *en de N-doorsnede over* $\mathrm{Rat}(N \times C)$ *semilineair zijn, dan is ook de $(M * N)$-doorsnede over* $\mathrm{Rat}((M * N) \times C)$ *semilineair.*

Bewijs: Zij $K, L \in \mathrm{Rat}((M * N) \times C)$. Omdat de commutatieve afbeeldingen bestaan, hebben monoïden M, N, C geen eenheidsdelers. Volgens Lemma 3.5 zijn dan K en L het resultaat van bipartiete automaten die voldoen aan Eigenschap 1 en waarvan de takken gelabeld zijn met rationele deelverzamelingen van $M \times C$ en $N \times C$. Laat $\mathcal{B}$ het (M, N)-product zijn van deze automaten. Volgens Lemma 3.4 geldt nu: $\mathcal{L}(\mathcal{B}) = K \overset{M*N}{\cap} L$. Bekijken we de (M, N)-productconstructie van $\mathcal{B}$, samen met het feit dat de takken van de bipartiete automaten van K en L gelabeld zijn met rationele deelverzamelingen, dan zien we dat de takken gelabeld zijn met verzamelingen die ontstaan door de M-doorsnede van rationele deelverzamelingen van $M \times C$ te nemen en de N-doorsnede van rationele deelverzamelingen van $N \times C$. Maar van deze verzamelingen weten we dat ze semilineair zijn. De commutatieve afbeelding van $\mathcal{L}(\mathcal{B})$ wordt dus gedefinieerd door een automaat over semilineaire verzamelingen en is daarom ook semilineair. $\Box$

Opgemerkt wordt dat we in de stelling ook hadden kunnen werken met monoïden M, N, en $M * N$, in plaats van $M \times C$, $N \times C$, en $(M * N) \times C$. Het bewijs gaat dan op dezelfde manier, neem $C = \{1\}$, waarbij we eventueel de $(M * N)$-doorsnede kunnen vervangen door de gewone doorsnede. Dit zou meer overeenkomen met het doel van de stelling, namelijk het bewijzen van een eigenschap van het vrije product. Het directe product met monoïde C hebben we echter nodig in Hoofdstuk 4 waar deze stelling wordt gebruikt in samenhang met de stelling uit de volgende paragraaf. Zie ook Appendix A.

3.3 De doorsnede en het directe product

We definiëren eerst de functie Move.

Definitie 3.7 *Laat* Σ, Δ_1, Δ_2 *disjuncte alfabets zijn. We definiëren de functie* $\mathrm{Move}_{\Delta_1} : \Sigma^{\oplus} \times (\Delta_1 \cup \Delta_2)^{\oplus} \times (\Delta_1 \cup \Delta_2)^{\oplus} \rightarrow (\Sigma \cup \Delta_1)^{\oplus} \times \Delta_2^{\oplus} \times \Delta_2^{\oplus}$ *als volgt:* $\mathrm{Move}_{\Delta_1}(\psi_1, \psi_2, \psi_3) = (\psi_1', \psi_2', \psi_3')$, *met* $\psi_1'(a) = \psi_1(a)$, *voor alle* $a \in \Sigma$, $\psi_1'(b) = \psi_2(b)$, *voor alle* $b \in \Delta_1$, *en* $\psi_2'(c) = \psi_2(c)$, $\psi_3'(c) = \psi_3(c)$, *voor alle* $c \in \Delta_2$.

Functie Move_{Δ_1} toegepast op tupel (ψ_1, ψ_2, ψ_3) verplaatst de waarden die ψ_2 geeft voor Δ_1 naar ψ_1. De waarden die ψ_3 geeft voor Δ_1 gaan verloren. Deze functie gaan we straks echter gebruiken in geval $\psi_2(a) = \psi_3(a)$, voor alle $a \in \Delta_1$.

Wanneer we functie Move toepassen op een semilineaire verzameling, dan is het resultaat weer semilineair.

Lemma 3.8 *Laat* Σ, Δ_1, Δ_2 *disjuncte alfabets zijn en* $S \subseteq \Sigma^{\oplus} \times (\Delta_1 \cup \Delta_2)^{\oplus} \times (\Delta_1 \cup \Delta_2)^{\oplus}$ *een semilineaire verzameling. De verzameling die ontstaat door functie* Move_{Δ_1} *op* S *toe te passen is semilineair.*

Bewijs: Zij $S' = \mathrm{Move}_{\Delta_1}(S)$. Omdat S semilineair is, bestaat er een reguliere expressie over $\Sigma^{\oplus} \times (\Delta_1 \cup \Delta_2)^{\oplus} \times (\Delta_1 \cup \Delta_2)^{\oplus}$ die S definieert. Door functie Move_{Δ_1} toe te passen op de tupels van deze expressie, krijgen we een reguliere expressie die S' definieert. Hieruit volgt dat S' ook semilineair is. $\Box$

De volgende stelling bewijst nu een cruciale eigenschap met betrekking tot monoïden die opgebouwd worden door middel van het directe product. In het bewijs hebben we functie Move nodig.

Stelling 3.9 *Laat* M, C_1, C_2 *disjuncte en eindig voortgebrachte monoïden zijn, waarvoor de commutatieve afbeeldingen bestaan, met de eis dat* C_1 *commutatief is. Als de* M*-doorsnede over* $\mathrm{Rat}(M \times C_1 \times C_2)$ *semilineair is, dan is ook de* $(M \times C_1)$*-doorsnede over* $\mathrm{Rat}(M \times C_1 \times C_2)$ *semilineair.*

Bewijs: Laat M eindig voortgebracht worden door Σ, C_1 door Δ_1, en C_2 door Δ_2. Zij $K, L \subseteq \mathrm{Rat}(M \times C_1 \times C_2)$, en $A = \{(\psi_1, \psi_2, \psi_3) \in \Sigma^{\oplus} \times (\Delta_1 \cup \Delta_2)^{\oplus} \times (\Delta_1 \cup \Delta_2)^{\oplus} \mid \psi_2(a) = \psi_3(a), \text{ voor alle } a \in \Delta_1\}$. Zij verder $B = \psi_{\Sigma, \Delta_1 \cup \Delta_2}(K \overset{M}{\cap} L) \cap A$. Omdat de M-doorsnede over $\mathrm{Rat}(M \times C_1 \times C_2)$ semilineair is, en semilineaire verzamelingen gesloten zijn onder doorsnede, geldt dat B semilineair is. We krijgen nu, wegens het feit dat C_1 commutatief is, dat $\psi_{\Sigma \cup \Delta_1, \Delta_2}(K \overset{M \times C_1}{\cap} L) = \mathrm{Move}_{\Delta_1}(B)$. Hieruit volgt, wegens Lemma 3.8, dat de $(M \times C_1)$-doorsnede over $\mathrm{Rat}(M \times C_1 \times C_2)$, semilineair is. $\Box$

We hadden in de stelling monoïde C_2 weg kunnen laten. Het bewijs gaat dan op dezelfde manier, neem $C_2 = \{1\}$. Het product met C_2 hebben we echter nodig wanneer we deze stelling, in samenhang met Stelling 3.6, herhaaldelijk toegepassen, zoals dit in het volgende hoofdstuk gebeurt. In het bewijs, zoals het er nu uitziet, is het directe product met monoïde C_1 daarentegen wel noodzakelijk. Zie ook Appendix A.

Hoofdstuk 4

De doorsnede over trace-monoïden

In dit hoofdstuk bewijzen we dat het doorsnedeprobleem voor rationele deelverzamelingen van trace-monoïden beslisbaar is wanneer de onafhankelijkheidsalfabet gevormd wordt door een transitief bos. Eerst kijken we echter naar een klasse van trace-monoïden waarvoor het doorsnedeprobleem onbeslisbaar is.

4.1 Een klasse van trace-monoïden waarvoor het doorsnedeprobleem onbeslisbaar is

Wanneer een trace-monoïde een onafhankelijkheidsrelatie heeft die gelijk is aan $\{\{\mathrm{a}, \mathrm{c}\}, \{\mathrm{a}, \mathrm{d}\}, \{\mathrm{b}, \mathrm{c}\}, \{\mathrm{b}, \mathrm{d}\}\}$, zie Figuur 4.1, dan is het doorsnedeprobleem over rationele deelverzamelingen onbeslisbaar. In Lemma 4.1 wordt dit bewezen. Hierbij wordt gebruik gemaakt van het begrip *Post Correspondentie Systeem* (PCS).

Een PCS is een 4-tupel (Σ, k, A, B), met Σ een alfabet, $k \geq 2$, en $A = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, $B = (\beta_1, \beta_2, \ldots, \beta_k)$, met $\alpha_i, \beta_j \in \Sigma^+$. Het PCS heeft een oplossing wanneer er een rij $(i_1, i_2, \ldots, i_n)$, met $n \geq 1$, en $1 \leq i_j \leq k$, bestaat zodanig dat $\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_n} = \beta_{i_1}\beta_{i_2}\cdots\beta_{i_n}$. We noemen zo'n rij een oplossing van het PCS. Het is bekend dat de vraag of een willekeurige PCS een oplossing heeft onbeslisbaar is. Zie bijvoorbeeld [14].

Daarnaast maken we in het bewijs, ter bevordering van de overzichtelijkheid, gebruik van het feit dat $M \simeq \{\mathrm{a}, \mathrm{b}\}^* \times \{\mathrm{c}, \mathrm{d}\}^*$.

Lemma 4.1 *Laat $M = \mathrm{M}(\Sigma, I)$ een trace-monoïde zijn, met $\Sigma = \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}\}$, en $I = \{\{\mathrm{a}, \mathrm{c}\}, \{\mathrm{a}, \mathrm{d}\}, \{\mathrm{b}, \mathrm{c}\}, \{\mathrm{b}, \mathrm{d}\}\}$. Het is onbeslisbaar voor willekeurige rationele deelverzamelingen van M of de doorsnede al dan niet leeg is.*