Technische Universität Dresden
Fachrichtung Mathematik

Institut für Algebra

Die Struktur der Monoide binärer Relationen auf endlichen Mengen

Diplomarbeit
zur Erlangung des ersten akademischen Grades

Diplommathematiker

vorgelegt von

Name: Jäschke | Vorname: Robert

geboren am: 20.10.1980 | in: Wolfen

Tag der Einreichung: 25. April 2005

Betreuer: Prof. Dr. rer. nat. habil. Reinhard Pöschel

Inhaltsverzeichnis

1. Grundlagen **3**
- A. Das Monoid der Booleschen Matrizen . . . 3
- B. Verbandstheorie Boolescher Matrizen . . . 5
- C. Permutationen . . . 12
- D. Äquivalenz Boolescher Matrizen . . . 13

2. Die Struktur der Elemente von $\mathbf{B}_n$ **14**
- A. Die Devadze-Typen . . . 14
- B. Reguläre Matrizen . . . 24
- C. Prime Matrizen . . . 27
- D. Magere Matrizen . . . 31

3. Erzeugendensysteme für Untermonoide von $\mathbf{B}_n$ **32**
- A. Das Monoid $\mathbf{S}_n$ aller Permutationen . . . 34
- B. Das von den regulären Matrizen erzeugte Untermonoid . . . 35
- C. Magere Matrizen mit maximalem Zeilen- und Spaltenrang . . . 39

4. Das Theorem von Devadze **42**

5. Ausblick **45**

Einleitung

Relationen und insbesondere binäre Relationen gehören zu den grundlegenden Elementen der Mathematik und sind in vielfältiger Form auch im täglichen Leben anzutreffen. Das Relationenprodukt, als Verallgemeinerung der Komposition von Abbildungen, bildet zusammen mit allen binären Relationen auf einer Menge ein Monoid, genannt *Monoid der binären Relationen*. Als mögliche Darstellungsform für binäre Relationen bieten sich gerichtete Graphen und insbesondere Boolesche Matrizen an, da sich mit letzteren Berechnungen einfach ausführen lassen.
Das Monoid aller binären Relationen wurde von zahlreichen Autoren untersucht. Für die vorliegende Arbeit besonders wichtig ist Zareckis Artikel „Die Halbgruppe der binären Relationen“ [Zar63], welcher die Verbindung zwischen besagtem Monoid und der Verbandstheorie (siehe z.B. [Bir67]) herstellt. Besonderes Interesse gebührt des weiteren den regulären Matrizen. Dabei gaben Kim und Roush ein Erzeugendensystem, bestehend aus vier Elementen, für das Untermonoid aller Booleschen Matrizen an [KR77] und Konieczny fand hinreichende und notwendige Bedingungen für das Enthaltensein einer Matrix in diesem Untermonoid [Kon02]. Ebenfalls eine Rolle spielen prime Matrizen [dCG80, dCG81] und Greensche Äquivalenzen in den Betrachtungen vieler Autoren.
Einen wichtigen Baustein in der Theorie des Monoids binärer Relationen stellt das *Theorem von Devadze* dar, welches 1968 veröffentlicht wurde. Darin gibt H. M. Devadze nicht nur minimale Erzeugendensysteme für die Halbgruppe aller binären Relationen an, sondern sagt auch, daß eines der von ihm angegebenen in jedem Erzeugendensystem für diese Halbgruppe enthalten ist. Damit ist die Struktur jedweden minimalen Erzeugendensystems durch das Theorem von Devadze festgelegt. Devadze veröffentlichte seinen Artikel ohne Beweis – der Artikel gilt jedoch als Referenz bei der Betrachtung von Erzeugendensystemen für das Monoid aller binären Relationen.
Ziel dieser Arbeit soll es sein, das Theorem von Devadze zu beweisen und die Struktur der Elemente des Erzeugendensystems zu untersuchen. Dahingehend erfolgt insbesondere eine Betrachtung der Faktoren bestimmter Boolescher Matrizen. Dies gibt uns die Möglichkeit, Aussagen über die Minimalität des Erzeugendensystems zu treffen und darüberhinaus weitere minimale Erzeugendensysteme auszuschließen.
Während die Größe des Erzeugendensystems für das Monoid aller binären Relationen mit der Anzahl der Elemente der Grundmenge wächst, läßt sich das Untermonoid aller regulären Relationen stets aus nur vier Elementen erzeugen. Der Beweis von Kim und Roush ist in dieser Arbeit enthalten, da die darin vorgeführte Konstruktionsidee Grundlage für ein Lemma von Konieczny zum Beweis des Theorems von Devadze ist.
Zunächst werden im ersten Kapitel die Grundlagen für die folgenden Abschnitte gelegt. Insbesondere betrachten wir die Zeilen und Spalten einer Matrix als Elemente des Verbandes der Booleschen Vektoren und vergegenwärtigen uns die verbandstheoretischen Ergebnisse von Zarecki.
Kapitel 2 führt die von Devadze definierten Typen für Boolesche Matrizen ein und untersucht deren Eigenschaften. Dabei sind vor allem die möglichen Faktoren dieser Matrizen von Interesse – deren Betrachtung ermöglicht Aussagen über die Minimalität und Einmaligkeit der Erzeugendensysteme. Außerdem werden reguläre, prime und magere

Elemente des Monoids aller Booleschen Matrizen untersucht.
Das darauffolgende Kapitel bildet eine wesentliche Grundlage für den Beweis des Theorems von Devadze. Neben einem minimalen Erzeugendensystem für die symmetrische Gruppe betrachten wir den Satz von Kim und Roush über das von den regulären Matrizen erzeugte Untermonoid sowie zwei Lemmata von Konieczny. Außerdem ermöglicht uns eine Betrachtung der Mindestanzahl primer Matrizen, eine Aussage über das Wachstum der Größe eines Erzeugendensystems zu treffen.
Schließlich erfolgt im vierten Kapitel mit Hilfe von Koniecznys Ergebnissen der Beweis des Satzes von Devadze.
Noch eine Anmerkung zu zitierten Lemmata und Sätzen sei gestattet: Vor diesen gibt eine kurze Bemerkung den Autor und die Quelle an. Wurde der zugehörige Beweis im wesentlichen übernommen oder weggelassen, so folgt die Quellenangabe fett gedruckt und in eckigen Klammern dem Wort „Lemma“ bzw. „Satz“.

1. Grundlagen

A. Das Monoid der Booleschen Matrizen

Ein grundlegender Begriff in der Mathematik ist der Begriff der binären Relation. Damit können Beziehungen zwischen den Elementen einer Menge hergestellt werden und darauf aufbauend Abbildungen definiert werden. In diesem Abschnitt werden die Begriffe *binäre Relation, Boolesche Matrix* sowie *Monoid* eingeführt.

1.1 Definition Sei M eine Menge und $\alpha \subseteq M \times M$. Dann ist α eine *binäre Relation auf* M.
Mit $\underline{B}_M$ bezeichnen wir die Menge aller binären Relationen auf M und mit $\underline{B}_n$ die Menge aller binären Relationen auf der Menge $\underline{n} := \{1, \ldots, n\} \subseteq \mathbb{N}$.

Da wir in der gesamten Arbeit stets nur endliche Mengen studieren, können wir unsere Betrachtung auch auf die Menge $\underline{n} = \{1, \ldots, n\}$ beschränken. Dies vereinfacht die Notation und macht vieles übersichtlicher. Im weiteren Verlauf sei daher n stets eine beliebige natürliche Zahl.

1.2 Definition Seien α und β binäre Relationen auf $\underline{n}$. Dann ist durch

$$\alpha\,;\beta := \{(i,j) \in \underline{n} \times \underline{n} \mid \exists k \in \underline{n} : (i,k) \in \alpha \text{ und } (k,j) \in \beta\}$$

eine binäre Operation auf der Menge der binären Relationen definiert, genannt *Relationenprodukt.*

1.3 Definition Sei M eine Menge und $\circ$ eine binäre Operation auf M. Falls für alle $a, b, c \in M$ das Assoziativgesetz $a \circ (b \circ c) = (a \circ b) \circ c$ gilt, dann ist $(M, \circ)$ eine *Halbgruppe.* Existiert zusätzlich ein $e \in M$, so daß für alle $a \in M$ gilt: $e \circ a = a \circ e = a$, dann ist $(M, \circ, e)$ ein *Monoid* mit dem *neutralen Element* e.

Für $\alpha, \beta, \gamma \in \underline{B}_n$ besagt sowohl $(i,j) \in (\alpha\,;\beta)\,;\gamma$ als auch $(i,j) \in \alpha\,;(\beta\,;\gamma)$, daß $k, l \in \underline{n}$ existieren, so daß $(i,k) \in \alpha$, $(k,l) \in \beta$ und $(l,j) \in \gamma$ gilt. Damit ist das Relationenprodukt assoziativ und $(\underline{B}_n, ;)$ eine Halbgruppe. Da $\underline{\Delta} := \{(i,i) \mid i \in \underline{n}\}$ ein neutrales Element bezüglich des Relationenproduktes ist, ist $(\underline{B}_n, ;, \underline{\Delta})$ sogar ein Monoid, das *Monoid* $\mathbf{B}_n$ *der binären Relationen auf* $\underline{n}$.

1.4 Bemerkung Mittels der Abbildung

$$^\bullet : \mathbf{O}_n^{(1)} \to \underline{\mathbf{B}}_n : f \mapsto f^\bullet := \{(i, f(i)) \mid i \in \underline{n}\}$$

ist ein injektiver Homomorphismus zwischen $\mathbf{O}_n^{(1)}$, dem Monoid aller einstelligen Funktionen auf $\underline{n}$, und $\underline{\mathbf{B}}_n$ gegeben [KHJ04]. Dabei wird jeder Funktion f ihr *Graph* $f^\bullet$ zugeordnet, welcher eine binäre Relation ist.
Insbesondere ist das Relationenprodukt zweier Graphen von Funktionen wieder ein Graph einer Funktion – das Relationenprodukt kann man als Verallgemeinerung der Komposition von Funktionen auffassen

1.5 Definition Sei mit B_n die Menge aller $(n \times n)$-Matrizen über der Booleschen Algebra $\underline{\mathbf{2}} = (\{0,1\}, \vee, \wedge, {}^c, 0, 1)$ bezeichnet. Dann definieren wir darauf für alle $\alpha, \beta \in B_n$ eine Matrizenmultiplikation $\gamma := \alpha \cdot \beta$ mit

$$\gamma_{ij} := \bigvee_{k \in \underline{n}} (\alpha_{ik} \wedge \beta_{kj}),$$

wobei $\vee$ und $\wedge$ die Operationen in der Booleschen Algebra sind, d.h. $a \vee b = \max\{a, b\}$ und $a \wedge b = \min\{a, b\}$ für $a, b \in \underline{\mathbf{2}}$. Meist lassen wir das Multiplikationszeichen $\cdot$ auch weg und schreiben statt $\alpha \cdot \beta$ nur $\alpha\beta$.
Die *Einheitsmatrix* $\Delta \in B_n$ ist diejenige Matrix, für die $\Delta_{ij} = 1 \iff i = j$ gilt. Die Matrix, die aus lauter Nullen besteht, heißt *Nullmatrix* und wird mit $\mathbf{0}$ bezeichnet.
Die so definierte Matrizenmultiplikation ist assoziativ, denn $\vee$ und $\wedge$ sind assoziativ und distributiv in der Booleschen Algebra und die Einheitsmatrix ist ein neutrales Element. Daher ist $(B_n, \cdot, \Delta)$ ein Monoid, welches wir als das *Monoid* $\mathbf{B}_n$ *der Booleschen* $(n \times n)$*-Matrizen* bezeichnen.

1.6 Bemerkung Wir können binäre Relationen und Boolesche Matrizen miteinander identifizieren, indem wir jeder binären Relation eine Boolesche Matrix zuordnen:

$$\Phi : \underline{\mathbf{B}}_n \to \mathbf{B}_n : \alpha \mapsto \Phi(\alpha) \quad \text{mit} \quad \forall i, j \in \underline{n} : \ (\Phi(\alpha))_{ij} = 1 : \iff \ (i, j) \in \alpha.$$

Dies ist nicht nur eine Bijektion zwischen $\underline{\mathbf{B}}_n$ und $\mathbf{B}_n$, sondern sogar ein Homomorphismus, denn neben $\Phi(\underline{\Delta}) = \Delta$ gilt für alle $\alpha, \beta \in \underline{\mathbf{B}}_n$:

$$\begin{aligned}
(\Phi(\alpha\,;\beta))_{ij} = 1 \quad &\iff \quad (i,j) \in \alpha\,;\beta \\
&\iff \quad \exists k \in \underline{n} : (i,k) \in \alpha \ \text{ und } \ (k,j) \in \beta \\
&\iff \quad \exists k \in \underline{n} : (\Phi(\alpha))_{ik} = 1 \ \text{ und } \ (\Phi(\beta))_{kj} = 1 \\
&\iff \quad \exists k \in \underline{n} : (\Phi(\alpha))_{ik} \wedge (\Phi(\beta))_{kj} = 1 \\
&\iff \quad \bigvee_{k \in \underline{n}} \Big((\Phi(\alpha))_{ik} \wedge (\Phi(\beta))_{kj} \Big) = 1 \\
&\iff \quad (\Phi(\alpha) \cdot \Phi(\beta))_{ij} = 1
\end{aligned}$$

Folglich können wir Boolesche Matrizen als eine Darstellungsform binärer Relationen auffassen und beide Monoide miteinander identifizieren. Im weiteren Verlauf der Arbeit werden wir fast ausschließlich diese Darstellungsform nutzen, da sie viele Betrachtungen vereinfacht.

1.7 Beispiel Ein erstes Beispiel soll den Zusammenhang zwischen den binären Relationen und den Booleschen Matrizen verdeutlichen. Sei $\alpha := \{(1,1), (1,2), (2,2), (2,4), (3,1), (3,4), (4,1), (4,2), (4,3)\}$. Dann ergibt $\Phi(\alpha)$ die nebenstehende Matrix.

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

1.8 Definition Sei $\alpha \in \underline{\mathbf{B}}_n$. Dann ist $\alpha^\top$ definiert durch $\alpha^\top := \{(j,i) \mid (i,j) \in \alpha\}$. Für ein $\beta \in \mathbf{B}_n$ ist analog $\beta^\top$ mit $(\beta^\top)_{ij} := 1 \iff \beta_{ji} = 1$ definiert und wird die *zu* β *transponierte Matrix* genannt.

Offensichtlich gilt für jede Relation $\alpha \in \underline{\mathbf{B}}_n$, daß $\Phi(\alpha^\top)$ gleich $\Phi(\alpha)^\top$ ist.

1.9 Definition Für $\alpha \in \mathbf{B}_n$ definieren wir:

$$\mathbf{B}_n\alpha := \{\beta\alpha \mid \beta \in \mathbf{B}_n\}, \quad \alpha\mathbf{B}_n := \{\alpha\beta \mid \beta \in \mathbf{B}_n\} \quad \text{und} \quad \mathbf{B}_n\alpha\mathbf{B}_n := \{\beta\alpha\gamma \mid \beta,\gamma \in \mathbf{B}_n\},$$

wobei $\mathbf{B}_n\alpha$ das *linksseitige* und $\alpha\mathbf{B}_n$ das *rechtsseitige Hauptideal von* α genannt wird. Damit seien auf $\mathbf{B}_n$ die folgenden binären Relationen definiert:

$$\begin{aligned}
\mathscr{R} &:= \{(\alpha,\beta) \in \mathbf{B}_n \times \mathbf{B}_n \mid \alpha\mathbf{B}_n = \beta\mathbf{B}_n\} \\
\mathscr{L} &:= \{(\alpha,\beta) \in \mathbf{B}_n \times \mathbf{B}_n \mid \mathbf{B}_n\alpha = \mathbf{B}_n\beta\} \\
\mathscr{D} &:= \{(\alpha,\beta) \in \mathbf{B}_n \times \mathbf{B}_n \mid \mathbf{B}_n\alpha\mathbf{B}_n = \mathbf{B}_n\beta\mathbf{B}_n\}.
\end{aligned}$$

Diese Relationen heißen *Greensche Äquivalenzen* (nach J. A. Green [Gre51]), denn wie man leicht sieht, sind dies Äquivalenzrelationen. Die entsprechenden Äquivalenzklassen bezeichnen wir als $\mathscr{R}$-, $\mathscr{L}$- und $\mathscr{D}$-Klassen.

In Worten besagt $\alpha\mathscr{R}\beta$ ($\alpha\mathscr{L}\beta$), daß α und β das gleiche rechtsseitige (linksseitige) Hauptideal erzeugen. Desweiteren gilt für die Komposition: $\mathscr{R};\mathscr{L} = \mathscr{L};\mathscr{R} = \mathscr{D}$ [CP61].

1.10 Definition Eine Teilmenge U einer Halbgruppe $(M,\circ)$ heißt *Unterhalbgruppe von* $(M,\circ)$, falls für alle $a,b \in U$ gilt: $a \circ b \in U$. Entsprechend heißt $U \subseteq M$ *Untermonoid von* $(M,\circ,e)$, falls $(M,\circ,e)$ ein Monoid ist und $e \in U$ sowie $a \circ b \in U$ für alle $a,b \in U$ gilt.

B. Verbandstheorie Boolescher Matrizen

In diesem Abschnitt betrachten wir Boolesche Vektoren, welche zusammen mit der komponentenweisen Kleinergleich-Ordnung einen Verband bilden. Wir fassen die Zeilen und Spalten von Booleschen Matrizen als Vektoren auf und betrachten die davon erzeugten Verbände.
Dabei verstehen wir unter einer *Ordnungsrelation* eine reflexive, antisymmetrische und transitive Relation. Die Kenntnis der Begriffe *kleinstes/größtes Element*, *untere/obere Schranke*, *Infimum/Supremum* und *unterer/oberer Nachbar* setzen wir ebenfalls voraus. Doch zunächst sei durch $\alpha \leq \beta :\iff \forall i,j \in \underline{n} : \alpha_{ij} \leq \beta_{ij}$ für $\alpha,\beta \in \mathbf{B}_n$ auf der Menge der Booleschen Matrizen eine binäre Relation definiert. Dies ist eine Ordnungsrelation auf $\mathbf{B}_n$.

1.11 Definition Mit $V_n := \{(v_1,\ldots,v_n) \mid v_i \in \{0,1\}, i = 1,\ldots,n\}$ werde die Menge aller n-elementigen *Booleschen Vektoren* bezeichnet.

Da die Einträge der Vektoren nur aus einzelnen Ziffern bestehen, können die Kommata auch weggelassen werden, ohne die Eindeutigkeit der Darstellung zu verletzten.

1.12 Definition Eine Menge M, zusammen mit einer Ordnungsrelation $\leq$ wird *geordnete Menge* genannt.
Existiert zu je zwei Elementen $a, b \in M$ einer geordneten Menge $(M, \leq)$ das Supremum $a \vee b$ und das Infimum $a \wedge b$, so heißt $(M, \leq)$ *verbandsgeordnet*.

Die Menge V_n zusammen mit der komponentenweise definierten Ordnung

$$u \leq v :\iff \forall i \in \underline{n} : u_i \leq v_i$$

(für $u, v \in V_n$) ist eine geordnete Menge.
In V_n existiert zu je zwei Elementen $u, v \in V_n$ das Supremum $u \vee v$ und das Infimum $u \wedge v$, wobei gilt:

$$\begin{aligned} u \vee v &= (u_1 \vee v_1, \ldots, u_n \vee v_n) \\ u \wedge v &= (u_1 \wedge v_1, \ldots, u_n \wedge v_n). \end{aligned}$$

Daher ist $(V_n, \leq)$ eine verbandsgeordnete Menge.
Jeder verbandsgeordneten Menge ist auf natürliche Weise ein weiteres algebraisches Objekt zugeordnet:

1.13 Definition Ein *Verband* $\mathbf{V}$ ist eine Menge V zusammen mit zwei Operationen

$$\begin{aligned} &\vee : V \times V \to V : (v, w) \mapsto v \vee w \quad \text{und} \\ &\wedge : V \times V \to V : (v, w) \mapsto v \wedge w \end{aligned}$$

für die folgende Gesetze für alle $u, v, w \in V$ gelten:

$$\begin{aligned} u \vee (v \vee w) &= (u \vee v) \vee w & \qquad u \wedge (v \wedge w) &= (u \wedge v) \wedge w \\ u \vee v &= v \vee u & \qquad u \wedge v &= v \wedge u \\ u \vee u &= u & \qquad u \wedge u &= u \\ u \vee (u \wedge v) &= u & \qquad u \wedge (u \vee v) &= u \end{aligned}$$

Zusammen mit den Operationen $\vee$ und $\wedge$ bildet V_n den *Verband* $\mathbf{V}_n$ *der Booleschen Vektoren*. Dabei gilt für alle $v, w \in \mathbf{V}_n$ die Äquivalenz: $v \leq w \iff w = v \vee w$.
Existiert in einer geordneten Menge zu jeder Teilmenge das Supremum und auch das Infimum, so heißt diese Menge *vollständig*. Der zugehörige Verband ist ein *vollständiger* Verband. Da wir in dieser Arbeit nur endliche Mengen betrachten, sind alle entsprechenden Verbände automatisch auch vollständig. Demnach sei für $\{v_1, \ldots, v_k\} \subseteq \mathbf{V}_n$ definiert: $\bigvee_{i \in \underline{k}} v_i := v_1 \vee v_2 \vee \ldots \vee v_n$.
Ein wichtiges Beispiel ist der *Potenzmengenverband* einer endlichen Menge M. Betrachtet man auf der Potenzmenge 2^M die Mengenoperationen Schnitt und Vereinigung, dann erhält man einen vollständigen Verband.

1.14 Definition Die Booleschen Vektoren mit genau einer Eins heißen *Einheitsvektoren* und werden mit $e^{(i)} \in \mathbf{V}_n$ $(i \in \underline{n})$ bezeichnet, wobei $e^{(i)}_j = 1 :\iff i = j$. Der Vektor, der nur aus Nullen besteht, heißt *Nullvektor* und wird mit $\mathbf{0}$ bezeichnet.

Der Nullvektor ist das kleinste Element des Verbandes $\mathbf{V}_n$, während der Vektor, der nur aus Einsen besteht, das größte Element von $\mathbf{V}_n$ ist.

1.15 Definition Sei $K \subseteq \mathbf{V}$. Dann ist K ein *Kernsystem in* $\mathbf{V}$, wenn K abgeschlossen ist unter beliebigen Suprema, d.h. wenn es alle Suprema von Teilmengen von K enthält.

Jedes Kernsystem $K \subseteq \mathbf{V}$ ist zusammen mit den Operationen

$$u \vee_K v := u \vee_{\mathbf{V}} v \quad \text{und} \quad u \wedge_K v := \bigvee\nolimits_{\mathbf{V}} \{w \in K \mid w \leq u \wedge_{\mathbf{V}} v\} \quad \text{für alle } u, v \in K$$

ein vollständiger Verband (wobei $\wedge_{\mathbf{V}}$ bzw. $\wedge_K$ das Infimum in $\mathbf{V}$ bzw. K ist, $\vee_{\mathbf{V}}$ und $\vee_K$ entsprechend das Supremum in $\mathbf{V}$ bzw. K). Denn neben dem Supremum, das per Definition für jede Teilmenge existiert, ergibt sich das Infimum einer beliebigen Teilmenge von K als Supremum aller Elemente, die unterhalb aller Elemente der Teilmenge liegen.

1.16 Definition Sei $\mathbf{V}$ ein Verband und $A \subseteq \mathbf{V}$. Dann bezeichnet $A^{\sup}$ die *Menge aller Suprema von Teilmengen von* A, ist also definiert als: $A^{\sup} := \{\bigvee_{x \in X} x \mid X \subseteq A\}$.

Wie man leicht sieht, ist diese Abbildung von $2^{\mathbf{V}}$ nach $2^{\mathbf{V}}$ für alle $A, B \subseteq \mathbf{V}$ extensiv $(A \subseteq A^{\sup})$ und isoton $(A \subseteq B \Rightarrow A^{\sup} \subseteq B^{\sup})$. Des weiteren folgt aus $A \subseteq A^{\sup}$ wegen der Isotonie: $A^{\sup} \subseteq (A^{\sup})^{\sup}$. Und es existiert für jedes $a \in (A^{\sup})^{\sup}$ ein $X \subseteq A^{\sup}$ mit $a = \bigvee_{x \in X} x$ und für jedes $x \in X$ ein $Y_x \subseteq A$ mit $x = \bigvee_{y \in Y_x} y$. Folglich gilt: $a = \bigvee_{x \in X} \bigvee_{y \in Y_x} y$ und a ist als Supremum von Elementen aus A in $A^{\sup}$ enthalten. Es gilt also $A^{\sup} = (A^{\sup})^{\sup}$ und damit ist diese Abbildung idempotent.
Das kleinste Element eines Verbandes ist für jedes $A \subseteq \mathbf{V}$ stets in $A^{\sup}$ enthalten. Denn das Supremum über die leere Menge ergibt das kleinste Element des Verbandes. Insbesondere ist die Menge $A^{\sup}$ nach Definition ein Kernsystem in $\mathbf{V}$ und damit ein vollständiger Verband.

1.17 Definition Ein Verband $\mathbf{V}$ heißt *distributiv*, falls für alle $u, v, w \in V$ folgende Gesetze gelten: $u \vee (v \wedge w) = (u \vee v) \wedge (u \vee w)$ und $u \wedge (v \vee w) = (u \wedge v) \vee (u \wedge w)$.

Der Potenzmengenverband einer endlichen Menge ist distributiv, ebenso der Verband der Booleschen Vektoren und beide Verbände sind zueinander isomorph (die Abbildung $2^{\underline{n}} \to \mathbf{V}_n : I \mapsto v : v_i = 1 :\iff i \in I$ ist ein Isomorphismus) .

1.18 Definition Sei $v \in \mathbf{V}_n$ und $\alpha \in \mathbf{B}_n$. Dann bezeichnet $|v|$ die Anzahl an Einsen von v und $|\alpha|$ die Anzahl an Einsen von α.

1.19 Definition Auf $\mathbf{V}_n$ sei folgende binäre Operation definiert:

$$\ominus : \mathbf{V}_n \times \mathbf{V}_n \to \mathbf{V}_n,\ u \ominus v \mapsto w, \quad \text{mit} \quad w_i = 1 :\iff u_i = 1 \text{ und } v_i = 0.$$

Betrachtet man für zwei Vektoren $u, v \in \mathbf{V}_n$ die Mengen $I_u := \{i \in \underline{n} \mid u_i = 1\}$ und $I_v := \{i \in \underline{n} \mid v_i = 1\}$, so ist $I_{u \ominus v}$ gleich $I_u \setminus I_v$. Diese Operation „löscht“ also in u jene Einsen, die auch in v „liegen“. Es gilt dann: $u = (u \ominus v) \vee v$.
Der Zusammenhang zwischen den Booleschen Matrizen als Darstellungsform binärer Relationen und den Booleschen Vektoren wird klarer, wenn man die Zeilen oder Spalten einer solchen Matrix untersucht. Deshalb definieren wir:

1.20 Definition Sei $\alpha \in \mathbf{B}_n$ und $i \in \underline{n}$. Dann bezeichnet α_{i*} die *i-te Zeile von* α, das heißt den Booleschen Vektor $(\alpha_{i1}, \ldots, \alpha_{in})$ und α_{*i} die *i-te Spalte von* α, also den Vektor $(\alpha_{1i}, \ldots, \alpha_{ni})$.

1.21 Definition Eine Zeile bzw. Spalte einer Matrix, die nur aus Nullen besteht, ist eine *Nullzeile* bzw. *Nullspalte*.

Die Zeilen und Spalten einer Booleschen Matrix sind Elemente von $\mathbf{V}_n$ und somit können wir die Operation $\vee$ anwenden:

1.22 Definition Sei $\alpha \in \mathbf{B}_n$. Dann ist der *Zeilenverband* $\mathfrak{Z}(\alpha)$ *von* α definiert als $\mathfrak{Z}(\alpha) := \{\alpha_{1*}, \alpha_{2*}, \ldots, \alpha_{n*}\}^{\sup} = \{\bigvee_{i \in I} \alpha_{i*} \mid I \subseteq \underline{n}\}$.

Das größte Element des Verbandes $\mathbf{V}_n$, der Vektor $(1, \ldots, 1)$, ist nicht zwingend im Zeilenverband einer Matrix enthalten, denn es werden nur alle Suprema von Teilmengen von Zeilen hinzugenommen, nicht die Infima ($(1, \ldots, 1)$ ist das Infimum der leeren Menge in $\mathbf{V}_n$).
In vielen englischsprachigen Arbeiten wird $\mathfrak{Z}(\alpha)$ auch als „row space“ bezeichnet. Die deutsche Übersetzung „Zeilenraum“ finde ich aber irreführend, da sie einen Zusammenhang zu Vektorräumen nahelegt. Aus der Definition geht jedoch unmittelbar hervor, daß $\mathfrak{Z}(\alpha)$ ein Kernsystem in $\mathbf{V}_n$ bildet und daher ein vollständiger Verband ist – die Bezeichnung Zeilen*verband* ist also gerechtfertigt.
Zu bemerken ist, daß der Zeilenverband nicht automatisch ein Unterverband von $\mathbf{V}_n$ ist, denn im allgemeinen unterscheidet sich das Infimum zweier Elemente im Zeilenverband vom Infimum der beiden Elemente in $\mathbf{V}_n$.

1.23 Definition Sei $\mathbf{V}$ ein vollständiger Verband. Ein $v \in \mathbf{V}$ heißt $\bigvee$*-irreduzibel*, falls $v \neq \bigvee\{x \in \mathbf{V} \mid x < v\}$ gilt. Ist v nicht $\bigvee$-irreduzibel, so nennen wir es auch $\bigvee$*-reduzibel*.

Der Nullvektor ist $\bigvee$-reduzibel in $\mathbf{V}_n$, denn $\bigvee \emptyset = \mathbf{0}$. Betrachten wir die $\bigvee$-irreduziblen Elemente von $\mathfrak{Z}(\alpha)$, so sind dies genau jene Zeilen, die sich nicht als Supremum anderer Zeilen aus $\mathfrak{Z}(\alpha)$ darstellen lassen. Da diese eindeutig bestimmt sind ist die folgende Definition sinnvoll:

1.24 Definition Sei $\alpha \in \mathbf{B}_n$. Dann bezeichnet die *Zeilenbasis* $\mathfrak{Z}_B(\alpha)$ *von* α die Menge der $\bigvee$-irreduziblen Elemente von $\mathfrak{Z}(\alpha)$.
Die Kardinalität $|\mathfrak{Z}_B(\alpha)|$ der Zeilenbasis erhält die Bezeichnung *Zeilenrang von* α. Der Zeilenrang einer Matrix ist *maximal*, falls er gleich n ist – die Zeilenbasis also alle Zeilen von α enthält.

Es stellt sich die Frage was ist, wenn $\alpha \in \mathbf{B}_n$ zwei gleiche Zeilen hat? Also $i, j \in \underline{n}$ mit $i \neq j$ existieren, so daß $\alpha_{i*} = \alpha_{j*}$ gilt. Da Zeilenverband und -basis *Mengen* sind, ist der Vektor α_{i*} höchstens einmal enthalten. Beide Mengen sind somit wohldefiniert. Die Zuordnung Zeile der Matrix zu Vektor des Zeilenverbandes (der Zeilenbasis) ist jedoch nicht injektiv. Darum muß man beim Schritt vom Zeilenverband zur zugehörigen Matrix beachten, daß man nicht zwingend eine eindeutig bestimmte Zeile erhält.
Des weiteren ist zu bemerken, daß jedes Element der Zeilenbasis eine Zeile der Matrix ist (sonst müßte es als Supremum von Zeilen der Matrix entstanden sein und wäre damit $\bigvee$-reduzibel) und die Supremum-irreduziblen Elemente des Verbandes $\mathbf{V}_n$ genau die Einheitsvektoren $e^{(i)}$ sind.

1.25 Beispiel Nachdem wir nun einige neue Begriffe kennengelernt haben, wollen wir uns diese an einem Beispiel veranschaulichen. Sei dazu $\alpha \in \mathbf{B}_n$ folgendermaßen definiert:

$$\alpha := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

Dann ist $\mathfrak{Z}(\alpha) = \{(0000), (1111), (1100), (0101), (1001), (1110), (1101)\}$ ein vollständiger Verband mit dem in Abbildung 1 dargestellten Hasse-Diagramm
Die $\bigvee$-irreduziblen Elemente des Zeilenverbandes, welche die Zeilenbasis bilden, sind: $\mathfrak{Z}_B(\alpha) = \{(1100), (0101), (1001), (1110)\}$.

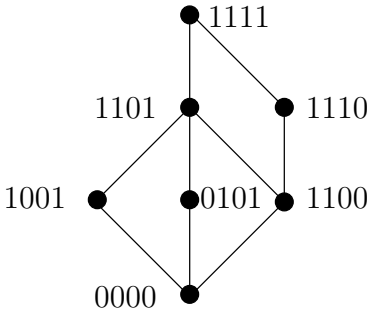


Abbildung 1: $\mathfrak{Z}(\alpha)$

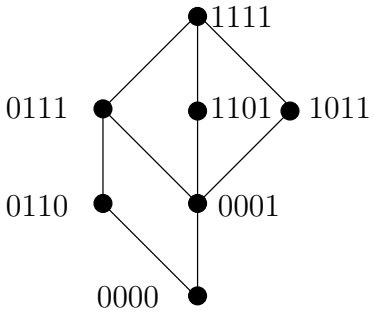


Abbildung 2: $\mathfrak{S}(\alpha)$

1.26 Definition Seien $A, B \subseteq \mathbf{V}$. Wenn $A^{\text{sup}} = B$ gilt, dann sagt man A *spannt* B *auf.*

1.27 Bemerkung Die Zeilenbasis spannt den Zeilenverband auf.
Weil die Abbildung $()^{\text{sup}}$ isoton und extensiv ist, reicht es zu zeigen, daß jede Zeile von α in $(\mathfrak{Z}_B(\alpha))^{\text{sup}}$ enthalten ist. Angenommen, dies gilt nicht. Dann definieren wir $A := \{\alpha_{1*}, \ldots, \alpha_{n*}\} \setminus (\mathfrak{Z}_B(\alpha))^{\text{sup}}$ und wählen $\alpha_{i*} \in A$ so, daß kein $\alpha_{j*} \in A$ echt kleiner als α_{i*} ist. Da α_{i*} nicht $\bigvee$-irreduzibel in $\mathfrak{Z}(\alpha)$ ist, existiert eine Menge $J \subseteq \underline{n}$ mit $\alpha_{i*} = \bigvee_{j \in J} \alpha_{j*}$, wobei alle α_{j*} echt kleiner als α_{i*} sind. Wären alle α_{j*} im Kernsystem

$(\mathfrak{Z}_B(\alpha))^{\sup}$ enthalten, so auch α_{i*}. Folglich ist eine der Zeilen α_{j*} echt kleiner als α_{i*} und in A enthalten – im Widerspruch zur Wahl von α_{i*}.

1.28 Bemerkung Die entsprechenden Begriffe für die *Spalten* einer Matrix $\alpha \in \mathbf{B}_n$ definieren wir analog und somit erhalten wir den *Spaltenverband* $\mathfrak{S}(\alpha)$, die *Spaltenbasis* $\mathfrak{S}_B(\alpha)$ und den *Spaltenrang* $|\mathfrak{S}_B(\alpha)|$.

Folglich ergibt sich für die Matrix aus Beispiel 1.25 auf der vorherigen Seite:

$$\begin{aligned}\mathfrak{S}(\alpha) &= \{(0000), (1111), (1011), (1101), (0001), (0110), (0111)\}\\ \mathfrak{S}_B(\alpha) &= \{(1011), (1101), (0001), (0110)\}.\end{aligned}$$

Das zugehörige Hasse-Diagramm für $\mathfrak{S}(\alpha)$ befindet sich in Abbildung 2 auf der vorherigen Seite.

1.29 Definition Eine Zeile α_{i*} von $\alpha \in \mathbf{B}_n$ heißt *minimal*, falls keine Zeile α_{j*} mit $i \neq j$ und $\alpha_{j*} \neq \mathbf{0}$ existiert, so daß $\alpha_{j*} \leq \alpha_{i*}$ gilt. Ebenso heißt eine Spalte α_{*k} *minimal*, falls keine Spalte α_{*l} $(l \neq k, \alpha_{*l} \neq \mathbf{0})$ mit $\alpha_{*l} \leq \alpha_{*k}$ existiert.

Die minimalen Elemente des Zeilen- bzw. Spaltenverbandes sind gerade die oberen Nachbarn des Nullvektors und der Nullvektor selbst.

1.30 Bemerkung Jede minimale Zeile α_{i*} von $\alpha \in \mathbf{B}_n$ mit $\alpha_{i*} \neq \mathbf{0}$ ist in der Zeilenbasis $\mathfrak{Z}_B(\alpha)$ enthalten. Ebenso ist jede minimale Spalte, die nicht der Nullvektor ist, in der Spaltenbasis enthalten.
Denn angenommen, $\alpha_{i*} \neq \mathbf{0}$ ist minimal, aber nicht $\bigvee$-irreduzibel. Dann existiert eine Menge $J \subseteq \underline{n}$ mit $\alpha_{i*} = \bigvee_{j\in J} \alpha_{j*}$ und es existiert ein $j \in J$ mit $\alpha_{j*} \neq \mathbf{0}$ und $\alpha_{j*} < \alpha_{i*}$, im Widerspruch zur Minimalität von α_{i*}. Analog zeigt man dies für die Spalten.

Das nachfolgende Lemma faßt einige der Ergebnisse von Zarecki [Zar63] zusammen, welche später von Plemmons und West [PW70] erweitert erweitert wurden. Insbesondere stellt es einen ersten Zusammenhang zwischen der verbandstheoretischen Sicht auf eine Boolesche Matrix (also Begriffen wie Zeilenverband und -basis) und dem Matrizenprodukt her.

1.31 Lemma *Für alle Matrizen $\alpha, \beta \in \mathbf{B}_n$ gilt:*

(1) $|\mathfrak{Z}(\alpha)| = |\mathfrak{S}(\alpha)|$

(2) $\mathfrak{Z}(\alpha) \subseteq \mathfrak{Z}(\beta) \iff$ *es existiert ein* $\gamma \in \mathbf{B}_n$ *mit* $\alpha = \gamma\beta$

(3) $\mathfrak{S}(\alpha) \subseteq \mathfrak{S}(\beta) \iff$ *es existiert ein* $\gamma \in \mathbf{B}_n$ *mit* $\alpha = \beta\gamma$

(4) $\alpha \mathscr{L} \beta \iff \mathfrak{Z}(\alpha) = \mathfrak{Z}(\beta) \iff \mathfrak{Z}_B(\alpha) = \mathfrak{Z}_B(\beta)$

(5) $\alpha \mathscr{R} \beta \iff \mathfrak{S}(\alpha) = \mathfrak{S}(\beta) \iff \mathfrak{S}_B(\alpha) = \mathfrak{S}_B(\beta)$

Beweis:

(1) In [Zar63] zeigt Zarecki sogar, daß $\mathfrak{Z}(\alpha)$ und $\mathfrak{S}(\alpha)$ isomorph sind. Aus diesem Beweis folgt sofort $|\mathfrak{Z}(\alpha)| = |\mathfrak{S}(\alpha)|$.

(2) „$\Rightarrow$“: Sei $\mathfrak{Z}(\alpha) \subseteq \mathfrak{Z}(\beta)$. Dann ist jede Zeile von α in $\mathfrak{Z}(\beta)$ enthalten und daher gilt: $\forall i \in \underline{n}\, \exists K_i \subseteq \underline{n} : \alpha_{i*} = \bigvee_{k \in K_i} \beta_{k*}$. Sei des weiteren die Matrix γ definiert als $\gamma_{ik} = 1 : \Longleftrightarrow\ \beta_{k*} \leq \alpha_{i*}$. Dann gilt einerseits

$$\begin{aligned}
(\gamma\beta)_{ij} = 1 \quad &\Rightarrow \quad \exists k \in \underline{n} : \gamma_{ik} = 1 \text{ und } \beta_{kj} = 1 \\
&\Rightarrow \quad \exists k \in \underline{n} : \beta_{k*} \leq \alpha_{i*} \text{ und } e^{(j)} \leq \beta_{k*} \\
&\Rightarrow \quad e^{(j)} \leq \alpha_{i*} \quad \Rightarrow \quad \alpha_{ij} = 1
\end{aligned}$$

und andererseits

$$\begin{aligned}
\alpha_{ij} = 1 \quad &\Rightarrow \quad e^{(j)} \leq \alpha_{i*} \\
&\Rightarrow \quad \exists K_i \subseteq \underline{n} : e^{(j)} \leq \bigvee_{k \in K_i} \beta_{k*} \quad (= \alpha_{i*}) \\
&\Rightarrow \quad \exists k \in \underline{n} : e^{(j)} \leq \beta_{k*} \text{ und } \beta_{k*} \leq \alpha_{i*} \\
&\Rightarrow \quad \exists k \in \underline{n} : \beta_{kj} = 1 \text{ und } \gamma_{ik} = 1 \quad \Rightarrow \quad (\gamma\beta)_{ij} = 1
\end{aligned}$$

und damit $\alpha_{ij} = 1 \Longleftrightarrow (\gamma\beta)_{ij} = 1$, also $\alpha = \gamma\beta$.

„$\Leftarrow$“: Es sei $\gamma \in \mathbf{B}_n$ mit $\alpha = \gamma\beta$, $i \in \underline{n}$ und $K_i := \{k \in \underline{n} \mid \gamma_{ik} = 1\}$. Dann gilt:

$$\begin{aligned}
\alpha_{ij} = 1 \quad &\Longleftrightarrow \quad (\gamma\beta)_{ij} = 1 \\
&\Longleftrightarrow \quad \exists k \in \underline{n} : \gamma_{ik} = 1 \text{ und } \beta_{kj} = 1 \\
&\Longleftrightarrow \quad \exists k \in K_i : \gamma_{ik} = 1 \text{ und } \beta_{kj} = 1 \\
&\Longleftrightarrow \quad \exists k \in K_i : \beta_{kj} = 1 \\
&\Longleftrightarrow \quad \bigvee_{k \in K_i} \beta_{kj} = 1
\end{aligned}$$

für alle $j \in \underline{n}$ und folglich für alle $i \in \underline{n}$:

$$\exists K_i \subseteq \underline{n} : \alpha_{i*} = \bigvee_{k \in K_i} \beta_{k*}.$$

Also ist jede Zeile von α in $\mathfrak{Z}(\beta)$ enthalten und somit gilt: $\{\alpha_{1*}, \ldots, \alpha_{n*}\} \subseteq \mathfrak{Z}(\beta)$ und mit der Isotonie und Idempotenz von $()^{\sup}$ schließlich: $\mathfrak{Z}(\alpha) \subseteq \mathfrak{Z}(\beta)$.

(3) Ist die gleiche Aussage wie (4) für die Spalten und wird analog bewiesen.

(4) Sei $\alpha \mathscr{L} \beta$. Dann existiert ein γ mit $\alpha = \gamma\beta$ und daher gilt nach (2): $\mathfrak{Z}(\alpha) \subseteq \mathfrak{Z}(\beta)$. Da außerdem ein δ existiert mit $\beta = \delta\alpha$ gilt auch $\mathfrak{Z}(\beta) \subseteq \mathfrak{Z}(\alpha)$ und damit $\mathfrak{Z}(\alpha) = \mathfrak{Z}(\beta)$.

Gilt andererseits $\mathfrak{Z}(\alpha) = \mathfrak{Z}(\beta)$, dann existieren nach (2) γ, δ mit $\alpha = \gamma\beta$ und $\beta = \delta\alpha$ und dann gilt: $\mathbf{B}_n\alpha = \mathbf{B}_n(\gamma\beta) \subseteq \mathbf{B}_n\beta$ und $\mathbf{B}_n\beta = \mathbf{B}_n(\delta\alpha) \subseteq \mathbf{B}_n\alpha$ und damit $\mathbf{B}_n\alpha = \mathbf{B}_n\beta$, also $\alpha \mathscr{L} \beta$.

Sind zwei Verbände gleich, so ist auch die Menge ihrer $\bigvee$-irreduziblen Elemente gleich. Da nach Bemerkung 1.27 auf Seite 9 die Zeilenbasis den Zeilenverband aufspannt, folgt andererseits, daß bei gleichen Zeilenbasen der Zeilenverband gleich ist. Demnach gilt die Äquivalenz: $\mathfrak{Z}(\alpha) = \mathfrak{Z}(\beta) \iff \mathfrak{Z}_B(\alpha) = \mathfrak{Z}_B(\beta)$.

(5) Ist die gleiche Aussage wie (4) für die Spalten und wird analog bewiesen. □

Bemerkung: Zarecki zeigt, daß (1), (2) und (3) sogar für den allgemeineren Fall von Booleschen $(m \times n)$-Matrizen gelten. Damit sind Anwendungen in der formalen Begriffsanalyse denkbar und in der Tat ist der Zeilenverband einer Booleschen Matrix isomorph zum Begriffsverband der entsteht, wenn man die komplementierte Matrix als formalen Kontext auffaßt. Die Aussage (1) enthält damit ein bekanntes Resultat der formalen Begriffsanalyse: die Anzahl der Begriffsumfänge ist gleich der Anzahl der Begriffsinhalte.

C. Permutationen

Einstellige injektive Abbildungen auf einer endlichen Menge bezeichnet man als *Permutationen*. Der Graph einer Permutation ist eine binäre Relation (siehe Bemerkung 1.4 auf Seite 3) und somit können wir Permutationen auch mit Elementen von $\mathbf{B}_n$ identifizieren. Die Menge aller Permutationen ist eine Gruppe und die Menge aller Permutationsmatrizen ein Untermonoid von $\mathbf{B}_n$, welches wir mit $\mathbf{S}_n$ bezeichnen. Die Begriffe Permutation und Permutationsmatrix werden wir oft synonym verwenden.
Diese Matrizen haben besondere Eigenschaften:

- Sie enthalten in jeder Zeile und in jeder Spalte genau eine Eins.
- Ist $\mu \in \mathbf{S}_n$ und $\alpha \in \mathbf{B}_n$, dann stellt $\mu\alpha$ eine Umordnung der Zeilen und $\alpha\mu$ eine Umordnung der Spalten von α dar. Dabei ändern sich Zeilenverband und Spaltenverband von α nicht.
- Da jede Zeile einer Permutationsmatrix ein Einheitsvektor und daher ein oberer Nachbar des Nullvektors ist, sind alle Zeilen minimal und somit in der Zeilenbasis enthalten (siehe Bemerkung 1.30 auf Seite 10). Der Zeilenrang ist also maximal und der Zeilenverband ist gleich $\mathbf{V}_n$ – gleiches gilt für Spaltenrang und -verband.

Sei $p \in \mathbf{O}_n^{(1)}$ eine Permutation. Dann existiert die zu p inverse Permutation p^{-1} und durch kurzes Nachrechnen sieht man, daß für die zu p gehörige Boolesche Matrix $\alpha := \Phi(p^\bullet)$ gilt: $\alpha^\top = \Phi((p^{-1})^\bullet)$. Zusammen mit den Bemerkungen 1.4 auf Seite 3 und 1.6 auf Seite 4 folgt dann:

$$\alpha^\top\alpha = \Phi((p^{-1}p)^\bullet) = \Phi((e_{\mathbf{O}_n^{(1)}})^\bullet) = \Delta = \Phi((pp^{-1})^\bullet) = \alpha\alpha^\top.$$

Demnach operiert für jede Permutationsmatrix α die transponierte Matrix $\alpha^\top$ als Inverses in $\mathbf{B}_n$, das heißt es gilt: $\alpha\alpha^\top = \alpha^\top\alpha = \Delta$.

1.32 Lemma *Sei $\alpha \in \mathbf{B}_n$. Dann ist α genau dann eine Permutationsmatrix, wenn für alle $\beta, \gamma \in \mathbf{B}_n$ mit $\alpha = \beta\gamma$ gilt: $\beta \in \mathbf{S}_n$ und $\gamma \in \mathbf{S}_n$.*

Beweis: Sei $\alpha \in \mathbf{S}_n$ und $\beta, \gamma \in \mathbf{B}_n$ mit $\alpha = \beta\gamma$. Jede Permutationsmatrix hat genau eine Eins in jeder Zeile und Spalte. Daher hat β keine Nullzeile und γ keine Nullspalte, denn sonst hätte α eine Nullzeile oder Nullspalte. Seien nun $i, j \in \underline{n}$ mit $\alpha_{ij} = 1$ gewählt. Dann existiert ein $k \in \underline{n}$ mit $\beta_{ik} = 1$ und $\gamma_{kj} = 1$. Angenommen, es existiert ein $b \in \underline{n}$ mit $b \neq i$ und $\beta_{bk} = 1$. Dann hätte α in der j-ten Spalte zwei Einsen (α_{ij} und α_{bj}) und wäre somit keine Permutationsmatrix. Deshalb kann β in jeder Spalte maximal eine Eins haben und analog zeigt man, daß γ in jeder Zeile maximal eine Eins haben darf. Damit hat β in jeder Zeile mindestens und in jeder Spalte höchstens eine Eins und ist daher eine Permutationsmatrix. Ebenso hat γ in jeder Spalte mindestens und in jeder Zeile höchstens eine Eins und ist ebenfalls eine Permutationsmatrix.
Die umgekehrte Richtung folgt aus der Tatsache, daß $\mathbf{S}_n$ ein Untermonoid von $\mathbf{B}_n$ ist und daher abgeschlossen bezüglich der Matrizenmultiplikation ist. □

Folgerung: Es folgt durch Induktion, daß das Lemma auch für Produkte mit mehr als zwei Faktoren gilt, das heißt α ist genau dann eine Permutationsmatrix, wenn für alle $\alpha_1, \ldots, \alpha_k \in \mathbf{B}_n$ mit $\alpha = \alpha_1 \cdot \ldots \cdot \alpha_k$ gilt: $\alpha_i \in \mathbf{S}_n$ $(i = 1, \ldots, k)$.

D. Äquivalenz Boolescher Matrizen

Um die Struktur des Monoids $\mathbf{B}_n$ zu untersuchen, werden wir bestimmte Elemente als einander „ähnlich“ erachten. Dabei ist uns die Anordnung der Zeilen und Spalten einer Matrix im wesentlichen egal – dies verändert ja auch den Zeilen- und Spaltenverband nicht. Infolgedessen definieren wir die Äquivalenz Boolescher Matrizen folgendermaßen:

1.33 Definition Zwei Matrizen $\alpha, \beta \in \mathbf{B}_n$ heißen *äquivalent*, wenn Permutationsmatrizen $\mu, \nu \in \mathbf{S}_n$ existieren, so daß $\alpha = \mu\beta\nu$ gilt. Wir schreiben dann auch $\alpha \cong \beta$ und sagen *α ist äquivalent zu β.*

1.34 Bemerkung Dies ist eine Äquivalenzrelation auf der Menge der Booleschen Matrizen, denn es gilt für alle $\alpha, \beta, \gamma \in \mathbf{B}_n$:

- $\alpha = \Delta\alpha\Delta$ (also $\alpha \cong \alpha$)
- $\alpha \cong \beta \quad \Rightarrow \quad \exists \mu, \nu \in \mathbf{S}_n : \alpha = \mu\beta\nu \quad \Rightarrow \quad \beta = \mu^\top \alpha \nu^\top \quad \Rightarrow \quad \beta \cong \alpha$
- $\alpha \cong \beta$ und $\beta \cong \gamma \quad \Rightarrow \quad \exists \mu, \nu, \kappa, \lambda \in \mathbf{S}_n : \alpha = \mu\beta\nu$ und $\beta = \kappa\gamma\lambda$
  $\Rightarrow \quad \alpha = \mu(\kappa\gamma\lambda)\nu = (\mu\kappa)\gamma(\lambda\nu) \quad \Rightarrow \quad \alpha \cong \gamma$

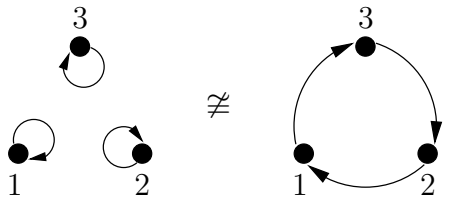
und damit Reflexivität, Symmetrie und Transitivität.

1.35 Bemerkung Faßt man für eine binäre Relation $\alpha \in \underline{\mathbf{B}}_n$ das Tupel $(\underline{n}, \alpha)$ als *gerichteten Graph* auf (d.h. $\underline{n}$ enthält die Knoten und α beschreibt gerichtete Kanten

zwischen den Knoten), dann kann man jede binäre Relation und damit jede Boolesche Matrix als Graph darstellen.
Betrachtet man die gerichteten Graphen zweier äquivalenter Matrizen, so sind diese nicht zwangsläufig isomorph. Das heißt die hier definierte Äquivalenzrelation $\cong$ auf der Menge der Booleschen Matrizen modelliert nicht die bekannte Isomorphie von Graphen. Ein Beispiel soll das verdeutlichen:

$$\alpha := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cong \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} =: \beta$$

Die gerichteten Graphen von α und β sind jedoch nicht isomorph:



2. Die Struktur der Elemente von $\mathbf{B}_n$

A. Die Devadze-Typen

In diesem Abschnitt werden wir bestimmten Matrizen einen *Typ* zuordnen und die Eigenschaften dieser Matrizen untersuchen. Devadze erkannte die Bedeutung dieser Booleschen Matrizen und teilte sie in Typen ein. Eine besondere Eigenschaft der zu betrachtenden Matrizen ist beispielsweise, daß man mit ihrer Hilfe andere Matrizen durch Multiplikation „verändern“ kann. So ist es möglich, Zeilen zu löschen oder durch andere Zeilen zu ersetzen.

2.1 Definition Seien $\tau, \pi, \varrho, \varrho' \in \mathbf{B}_n$ und

- τ enthalte genau $n+1$ Einsen mit $\tau_{ii} = 1$ für jedes $i \in \underline{n}$,
- π enthalte genau $n-1$ Einsen auf der Hauptdiagonale und allen anderen Einträge seien gleich Null,
- ϱ enthalte genau n Einsen und genau eine Nullzeile, aber keine Nullspalte,
- ϱ' enthalte genau n Einsen und genau eine Nullspalte, aber keine Nullzeile.

Jede zu $\begin{cases} \tau \\ \pi \\ \varrho \\ \varrho' \end{cases}$ äquivalente Matrix heißt Matrix vom *Typ* $\begin{cases} t \\ p \\ r \\ r' \end{cases}$.

2.2 Beispiel In der nachfolgenden Übersicht sind für $n = 5$ jeweils eine Matrix für jeden Typ und darunter die dazugehörigen gerichteten Graphen abgebildet.

Typ t

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Typ p

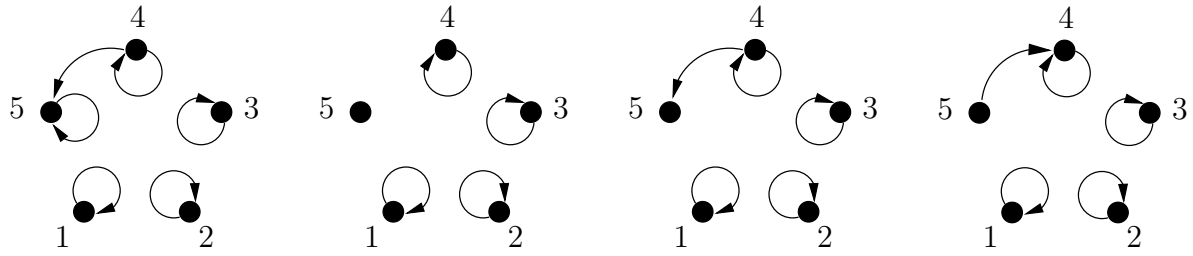
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Typ r

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Typ r′

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$



Die Matrizen im vorangegangenen Beispiel stellen für $n = 5$ einen Spezialfall „besonders übersichtlicher“ Matrizen für jeden Typ dar. Darum geben wir ihnen für beliebiges n einen Namen:

2.3 Definition Die Matrizen $\tau, \pi, \varrho, \varrho' \in \mathbf{B}_n$ seien wie folgt definiert:

$$\begin{aligned} \tau_{ij} = 1 &\iff i = j \text{ oder } (i,j) = (n-1, n) \\ \pi_{ij} = 1 &\iff i = j \text{ und } i \neq n \\ \varrho_{ij} = 1 &\iff (i = j \text{ und } i \neq n) \text{ oder } (i,j) = (n-1, n) \\ \varrho'_{ij} = 1 &\iff (i = j \text{ und } i \neq n) \text{ oder } (i,j) = (n, n-1) \end{aligned}$$

Die kleinen griechischen Buchstaben entsprechen dabei gerade dem Typ der Matrix. Auf den nachfolgenden Seiten sind mit τ, π, ϱ und ϱ' stets diese vier Matrizen gemeint.

2.4 Definition Sei für $k, l \in \underline{n}$ mit $k \neq l$ die Matrix $I^{kl} \in \mathbf{B}_n$ wie folgt definiert:

$$(I^{kl})_{ij} = 1 : \iff (i = j \text{ und } i \neq k \text{ und } i \neq l) \text{ oder } (i,j) = (k,l) \text{ oder } (i,j) = (l,k).$$

Für diese Matrizen gilt $(I^{kl})^\top = I^{kl}$ und weil dies Permutationen sind sogar: $I^{kl} I^{kl} = \Delta$. Multipliziert man ein $\alpha \in \mathbf{B}_n$ von links mit I^{kl}, so erhält man eine Matrix, die identisch ist zu α außer, daß die k-te mit der l-ten Zeile vertauscht wurde. Analog kann man in einer Matrix zwei Spalten miteinander vertauschen, wenn man sie von rechts mit einer geeigneten I^{kl}-Matrix multipliziert.
Die ursprüngliche Definition der Typen, die Devadze in seiner Arbeit [Dev68] angibt, schließt die äquivalenten Matrizen nicht ein. Für viele Lemmata ist es aber einfacher,

nicht nur die speziellen Matrizen eines Typs zu betrachten, sondern die dazu äquivalenten Matrizen hinzuzunehmen. Des weiteren könnten alle Matrizen eines Typs untereinander äquivalent sein. Daß dem tatsächlich so ist, beweist das folgende Lemma, welches die Betrachtung der Matrizen eines Typs erheblich vereinfacht.

2.5 Lemma *Alle Matrizen eines Typs sind äquivalent.*

Beweis: Wir zeigen, daß jede Matrix eines Typs äquivalent zur entsprechenden Matrix aus Definition 2.3 auf der vorherigen Seite ist. Wegen der Transitivität der Relation $\cong$ sind damit alle Matrizen eines Typs äquivalent.
Sei $\alpha \in \mathbf{B}_n$ vom Typ t. Zunächst ist α nach Definition äquivalent zu einer Matrix mit $n+1$ Einsen, wobei sich n dieser Einsen auf der Hauptdiagonale befinden. Das heißt es existieren $k, l \in \underline{n}\ (k \neq l)$ und $\beta \in \mathbf{B}_n$ mit $\beta_{ij} = 1 \iff i = j$ oder $(i,j) = (k,l)$, so daß $\alpha \cong \beta$ gilt.
Zu zeigen bleibt also, daß $\beta \cong \tau$ gilt, denn dann ist auch $\alpha \cong \tau$. Wir multiplizieren β von beiden Seiten mit der Matrix I^{ln}, wodurch die n-te und l-te Zeile und die n-te und l-te Spalte von β vertauscht werden:

$$I^{ln}\beta I^{ln} = I^{ln} \begin{array}{c} \\ 1 \\ \\ k \\ \\ l \\ \\ n \end{array} \begin{array}{c} \begin{array}{cccccccc} 1 & & & k & & l & & n \end{array} \\ \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & & 0 \\ \vdots & & \ddots & 1 & \ddots & 1 & & 0 \\ \vdots & & & \ddots & \ddots & \ddots & & 0 \\ \vdots & & & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & 1 \end{pmatrix} \end{array} I^{ln} = \begin{array}{c} \\ 1 \\ \\ k \\ \\ l \\ \\ n \end{array} \begin{array}{c} \begin{array}{cccccccc} 1 & & & k & & l & & n \end{array} \\ \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & & 0 \\ \vdots & & \ddots & 1 & \ddots & 0 & & 1 \\ \vdots & & & \ddots & \ddots & \ddots & & 0 \\ \vdots & & & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & 1 \end{pmatrix} \end{array}$$

Eine anschließende Multiplikation von beiden Seiten mit $I^{k,n-1}$ bringt schließlich das gewünschte Ergebnis:

$$I^{k,n-1}I^{ln}\beta I^{ln}I^{k,n-1} = \begin{array}{c} \\ 1 \\ \\ k \\ \\ l \\ \\ n-1 \\ n \end{array} \begin{array}{c} \begin{array}{cccccccccc} 1 & & & k & & l & & & n-1 & n \end{array} \\ \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & & & & 0 \\ \vdots & & \ddots & 1 & \ddots & 0 & & & & 0 \\ \vdots & & & \ddots & \ddots & \ddots & & & & 0 \\ \vdots & & & & \ddots & 1 & \ddots & & & \vdots \\ \vdots & & & & & \ddots & \ddots & \ddots & & 0 \\ \vdots & & & & & & \ddots & 1 & 1 & \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & \end{pmatrix} \end{array} = \tau$$

Damit ist jede Matrix vom Typ t äquivalent zu τ.
Für die Matrizen des Typs p funktioniert der Beweis auf ähnliche Art und Weise, denn nach Definition ist jede Typ p Matrix α äquivalent zu einer Matrix β mit genau $n-1$

Einsen auf der Hauptdiagonale und allen sonstigen Einträgen gleich Null. Daher hat β einen Eintrag $\beta_{kk} = 0$. Ist $k \neq n$, so multipliziert man β von links und von rechts mit I^{kn} und erhält die Matrix π, die somit äquivalent zu jeder Matrix vom Typ p ist.
Entsprechend dem bisher Gezeigten, kann man auch für jede Matrix α vom Typ r zeigen, daß α zu ϱ äquivalent ist. Dazu macht man durch Zeilenvertauschung die Nullzeile von α zur letzten Zeile und die Zeile mit den zwei Einsen zur vorletzten Zeile. Danach kann man zwei Spalten so tauschen, daß $\alpha_{n-1,n} = 1$ ist. Schließlich erhält man durch korrektes Vertauschen der ersten $n-1$ Spalten die Matrix ϱ. Da alle Zeilen- und Spaltenvertauschungen durch Links- und Rechtsmultiplikation mit geeigneten Permutationsmatrizen erreicht werden, ist α, und somit jede Matrix vom Typ r, äquivalent zu ϱ. Der Beweis für den Typ r′ funktioniert analog, d.h. jede Matrix vom Typ r′ ist äquivalent zu ϱ'. □

2.6 Bemerkung Schon aus der Definition der Typen folgt, daß beispielsweise für ein α vom Typ t und β mit $\alpha \cong \beta$ die Matrix β ebenfalls vom Typ t ist (entsprechend für die anderen Typen).
Somit bilden alle Matrizen eines Typs jeweils eine Äquivalenzklasse von $\cong$ und daher bietet es sich an, die Mengen $\mathcal{T}$, $\mathcal{P}$, $\mathcal{R}$ und $\mathcal{R}'$ wie folgt zu definieren:

$$\mathcal{T} := \{\alpha \in \mathbf{B}_n \mid \alpha \cong \tau\} \qquad \mathcal{P} := \{\alpha \in \mathbf{B}_n \mid \alpha \cong \pi\}$$
$$\mathcal{R} := \{\alpha \in \mathbf{B}_n \mid \alpha \cong \varrho\} \qquad \mathcal{R}' := \{\alpha \in \mathbf{B}_n \mid \alpha \cong \varrho'\}.$$

Demnach enthält $\mathcal{T}$ alle Matrizen vom Typ t und $\mathcal{P}$ alle vom Typ p und so weiter.

2.7 Bemerkung Es gilt $\varrho^\top = \varrho'$ und einfaches Nachrechnen zeigt, daß $\varrho\varrho' = \pi$ gilt. Aus einer Matrix vom Typ r und einer Matrix vom Typ r′ erhält man also durch Multiplikation mit geeigneten Permutationen die Matrizen ϱ und ϱ' und dadurch auch π.

2.8 Definition Sei für $k, l \in \underline{n}$ mit $k \neq l$ die Matrix $T^{kl} \in \mathbf{B}_n$ wie folgt definiert:

$$(T^{kl})_{ij} = 1 :\Longleftrightarrow\ i = j \ \text{ oder } \ (i,j) = (k,l).$$

2.9 Bemerkung Für alle $k, l \in \underline{n}$ mit $k \neq l$ sind die Matrizen T^{kl} vom Typ t. Durch Linksmultiplikation einer Matrix $\alpha \in \mathbf{B}_n$ mit T^{kl} ersetzt man die k-te Zeile von α durch das Supremum der k-ten mit der l-ten Zeile von α:

$$\beta := T^{kl}\alpha = \begin{pmatrix} \alpha_{1*} \\ \vdots \\ \alpha_{k-1*} \\ \alpha_{k*} \vee \alpha_{l*} \\ \alpha_{k+1*} \\ \vdots \\ \alpha_{n*} \end{pmatrix}.$$

Denn für β_{ij} mit $i \neq k$ gilt

$$\beta_{ij} = \bigvee_{h \in \underline{n}} ((T^{kl})_{ih} \wedge \alpha_{hj}) = (T^{kl})_{ii} \wedge \alpha_{ij} = \alpha_{ij}$$

und für β_{kj} gilt

$$\beta_{kj} = \bigvee_{h \in \underline{n}} ((T^{kl})_{kh} \wedge \alpha_{hj}) = ((T^{kl})_{kk} \wedge \alpha_{kj}) \vee ((T^{kl})_{kl} \wedge \alpha_{lj}) = \alpha_{kj} \vee \alpha_{lj}$$

und damit $\beta_{k*} = \alpha_{k*} \vee \alpha_{l*}$.
Etwas salopp gesagt, ist es mit den Matrizen T^{kl} möglich, die Zeilen einer anderen Booleschen Matrix „aufzuaddieren“. Natürlich ist mit Addieren nicht die übliche Addition, sondern das Bilden des Supremums im Zeilenverband gemeint, aber mangels eines entsprechenden Verbs werden wir dafür auch das Wort „addieren“ benutzen.
Multipliziert man eine Matrix α von rechts mit T^{kl}, so enthält die l-te Spalte der Ergebnismatrix das Supremum der k-ten mit der l-ten Spalte von α. Durch Rechtsmultiplikation kann man also die Spalten „aufaddieren“.

2.10 Definition Sei für $k \in \underline{n}$ die Matrix $P^k \in \mathbf{B}_n$ wie folgt definiert:

$$(P^k)_{ij} = 1 : \Longleftrightarrow \ i = j \ \text{ und } \ i \neq k$$

2.11 Bemerkung Für alle $k \in \underline{n}$ sind die Matrizen P^k vom Typ p. Multipliziert man eine Matrix $\alpha \in \mathbf{B}_n$ von links mit P^k, so erhält man eine zu α identische Matrix, in der jedoch die k-te Zeile „gelöscht“, d.h. durch den Nullvektor ersetzt, wurde.
Entsprechend kann man die k-te Spalte von α „löschen“, indem man α von rechts mit P^k multipliziert.

2.12 Bemerkung Sei $\alpha \in \mathbf{B}_n$ eine Matrix, die in jeder Zeile und in jeder Spalte maximal eine Eins enthält. Enthält α genau n Einsen, so ist es eine Permutation, enthält es genau $n-1$ Einsen, so ist es vom Typ p. Wenn α weniger als $n-1$ Einsen enthält, so läßt es sich stets als Produkt von Matrizen des Typs p darstellen.
Dazu wählt man als ersten Faktor eine Matrix $\beta \in \mathbf{B}_n$ vom Typ p, für die $\alpha \leq \beta$ gilt. Für jede Nullzeile α_{i*} in α multipliziert man β dann von links mit der Typ p Matrix P^i und erhält schließlich die Matrix α.

Das folgende Lemma trifft eine Aussage über die Faktoren einer Booleschen Matrix mit einer besonders einfachen Form: betrachten wir nur die ersten $n-1$ Zeilen und Spalten, so erhalten wir eine Permutationsmatrix. Die Faktoren sehen „im wesentlichen“ genauso aus, das heißt es existieren jeweils äquivalente Matrizen, welche die gleiche Form wie die Ausgangsmatrix haben.

2.13 Lemma *Sei $\alpha \in \mathbf{B}_n$ von folgender Form (wobei die Sterne „$*$“ beliebig, d.h. 0 oder 1 sein können):*

$$\alpha = \begin{pmatrix} \ulcorner & & \urcorner & * \\ & \tilde{\alpha} & & \vdots \\ \llcorner & & \lrcorner & * \\ * & \dots & * & * \end{pmatrix}$$

mit der $(n-1) \times (n-1)$ Einheitsmatrix $\tilde{\alpha}$. Wenn für $\beta, \gamma \in \mathbf{B}_n$ gilt $\alpha = \beta\gamma$, dann existiert ein $k \in \underline{n}$, so daß βI^{kn} und $I^{kn}\gamma$ die Gestalt

$$\beta I^{kn} = \begin{pmatrix} \ulcorner & & \urcorner & * \\ & \tilde{\beta} & & \vdots \\ \llcorner & & \lrcorner & * \\ * & \dots & * & * \end{pmatrix}, \quad I^{kn}\gamma = \begin{pmatrix} \ulcorner & & \urcorner & * \\ & \tilde{\gamma} & & \vdots \\ \llcorner & & \lrcorner & * \\ * & \dots & * & * \end{pmatrix}$$

haben, wobei $\tilde{\beta}$ und $\tilde{\gamma}$ Matrizen aus $\mathbf{S}_{n-1}$ sind.
Insbesondere gilt $(\beta I^{kn})(I^{kn}\gamma) = \beta\gamma = \alpha$ und βI^{kn} und β sind vom gleichen Typ und γI^{kn} und γ sind vom gleichen Typ (falls sie von einem der in 2.1 auf Seite 14 definierten Typen sind).

Beweis: Sei $\alpha = \beta\gamma$ eine Zerlegung von α in Faktoren und die $(n-1) \times n$ Matrix $\hat{\beta}$ sei definiert durch $\hat{\beta}_{i*} := \beta_{i*}$ für $i \in \underline{n-1}$. Analog sei die $n \times (n-1)$ Matrix $\hat{\gamma}$ definiert durch $\hat{\gamma}_{*j} := \gamma_{*j}$ für $j \in \underline{n-1}$. Die Matrizen $\hat{\beta}$ und $\hat{\gamma}$ ergeben sich also folgendermaßen:

$$\beta = \begin{pmatrix} \ulcorner & & \urcorner \\ & \hat{\beta} & \\ \llcorner & & \lrcorner \\ * & \dots & * \end{pmatrix}, \quad \gamma = \begin{pmatrix} \ulcorner & & \urcorner & * \\ & \hat{\gamma} & & \vdots \\ \llcorner & & \lrcorner & * \end{pmatrix}.$$

Dann enthält $\hat{\beta}$ keine Nullzeile und $\hat{\gamma}$ keine Nullspalte, denn sonst hätte $\tilde{\alpha}$ eine Nullzeile oder Nullspalte und wäre somit keine Permutationsmatrix. Also hat $\hat{\beta}$ in jeder Zeile und $\hat{\gamma}$ in jeder Spalte mindestens eine Eins.
Für jedes $i \in \underline{n-1}$ existiert ein $\tilde{\alpha}_{ii} = 1$ und damit auch ein $k_i \in \underline{n}$ mit $\hat{\beta}_{ik_i} = 1$ und $\hat{\gamma}_{k_i i} = 1$. So sei das $(n-1)$-Tupel K definiert als $K := (k_1, \dots, k_{n-1})$. Da für $i \neq j$ auch $k_i \neq k_j$ gilt (denn sonst wäre wegen $\hat{\beta}_{ik_i} = 1 = \hat{\gamma}_{k_j j}$ auch $\tilde{\alpha}_{ij} = 1$), sind die k_i alle paarweise verschieden. Die Matrix $\tilde{\alpha}$ wird also von den Spalten $\hat{\beta}_{*k_i}$ und Zeilen $\hat{\gamma}_{k_i *}$ „erzeugt“. Im $(n-1)$-Tupel K „merken“ wir uns die Stellen in den Zeilen und Spalten von $\hat{\beta}$ und $\hat{\gamma}$, an denen Einsen stehen.
Jede Spalte $\hat{\beta}_{*k_i}$ und jede Zeile $\hat{\gamma}_{k_i *}$ enthält außerdem genau eine Eins (an der Stelle $\hat{\beta}_{ik_i}$ bzw. $\hat{\gamma}_{k_i i}$). Denn angenommen, es existiert ein $j \in \underline{n-1}$ mit $j \neq i$ und $\hat{\beta}_{jk_i} = 1$ ($\hat{\gamma}_{k_i j} = 1$). Dann wäre $\tilde{\alpha}_{ji} = 1$ ($\tilde{\alpha}_{ij} = 1$), im Widerspruch zu $\tilde{\alpha}_{ij} = 1 \iff i = j$. Andererseits haben wir die $\hat{\beta}_{*k_i}$ und $\hat{\gamma}_{k_i *}$ ja gerade so gewählt, daß sie mindestens eine Eins enthalten.

Des weiteren existiert genau ein $k \in \underline{n}$ mit $k \neq k_i$ für alle $i \in \underline{n-1}$. Vertauschen wir in $\hat{\beta}$ die Spalten $\hat{\beta}_{*k}$ und $\hat{\beta}_{*n}$, so bilden die ersten $n-1$ Spalten die $(n-1) \times (n-1)$ Permutationsmatrix $\tilde{\beta}$. Ebenso erhalten wir durch Vertauschen der Zeilen $\hat{\gamma}_{k*}$ und $\hat{\gamma}_{n*}$ aus den ersten $n-1$ Zeilen die $(n-1) \times (n-1)$ Permutationsmatrix $\tilde{\gamma}$. Da ein solcher Spaltentausch (Zeilentausch) durch Multiplikation der Matrix I^{kn} von rechts an β (links an γ) erfolgt, hat die Matrix βI^{kn} ($I^{kn}\gamma$) die geforderte Struktur.
Wegen $I^{kn}I^{kn} = \Delta$, folgt $(\beta I^{kn})(I^{kn}\gamma) = \beta(I^{kn}I^{kn})\gamma = \beta\gamma = \alpha$ und da $I^{kn} \in \mathbf{S}_n$ gilt, folgt sofort $\beta = \Delta\beta(I^{kn}I^{kn}) = \Delta(\beta I^{kn})I^{kn}$ und damit $\beta \cong \beta I^{kn}$ (und analog $\gamma \cong I^{kn}\gamma$). Weil die Matrizen eines Typs paarweise äquivalent sind, ist folglich β vom selben Typ wie βI^{kn} und γ ist vom selben Typ wie $I^{kn}\gamma$. □
Eine erste Anwendung des vorhergehenden Lemmas ermöglicht uns, eine Aussage über den Typ der Faktoren einer Matrix vom Typ p zu treffen:

2.14 Lemma *Es sei $\alpha \in \mathbf{B}_n$ vom Typ p und $\beta, \gamma \in \mathbf{B}_n$ mit $\alpha = \beta\gamma$. Dann gilt:*

- *β ist vom Typ r und γ ist vom Typ r′ oder*
- *β ist vom Typ p oder γ ist vom Typ p.*

Beweis: Wir zeigen zunächst, daß für $\delta, \epsilon \in \mathbf{B}_n$ mit $\pi = \delta\epsilon$ ein $k \in \underline{n}$ existiert, so daß gilt:

- δI^{kn} ist vom Typ r und $I^{kn}\epsilon$ ist vom Typ r′ oder
- δI^{kn} ist vom Typ p oder $I^{kn}\epsilon$ ist vom Typ p.

Sei π wie in 2.1 auf Seite 14 definiert und $\pi = \delta\epsilon$ eine Faktorisierung von π. Dann existiert nach Lemma 2.13 auf Seite 18 ein $k \in \underline{n}$, so daß δI^{kn} und $I^{kn}\epsilon$ die folgende Gestalt haben:

$$\bar{\delta} := \delta I^{kn} = \begin{pmatrix} \ulcorner & & \urcorner & * \\ & \tilde{\delta} & & \vdots \\ \llcorner & & \lrcorner & * \\ * & \dots & * & * \end{pmatrix}, \quad \bar{\epsilon} := I^{kn}\epsilon = \begin{pmatrix} \ulcorner & & \urcorner & * \\ & \tilde{\epsilon} & & \vdots \\ \llcorner & & \lrcorner & * \\ * & \dots & * & * \end{pmatrix},$$

wobei $\tilde{\delta}, \tilde{\epsilon} \in \mathbf{S}_{n-1}$ sind.
Dann gilt für $i \in \underline{n-1}$: $\bar{\delta}_{ni} = 0$ und $\bar{\epsilon}_{in} = 0$, denn ansonsten gäbe es in der n-ten Zeile oder n-ten Spalte von π einen Eintrag ungleich Null, weil $\tilde{\delta}$ und $\tilde{\epsilon}$ in jeder Zeile bzw. Spalte mindestens eine Eins haben.
Betrachten wir jetzt die n-te Spalte von $\bar{\delta}$ und führen eine Fallunterscheidung durch:

$\underline{\bar{\delta}_{nn} = 1}$: Dann darf die n-te Zeile von $\bar{\epsilon}$ keine Eins enthalten, denn sonst hätte π in der n-ten Zeile eine Eins. Damit ist $\bar{\epsilon}$ vom Typ p.

$\underline{\bar{\delta}_{nn} = 0}$: Es gibt drei Möglichkeiten:

$\underline{\bar{\delta}_{*n} = \mathbf{0}}$: Dann ist $\bar{\delta}$ vom Typ p.

$\underline{\exists! h < n : \bar{\delta}_{hn} = 1}$: Dann muß $\bar{\epsilon}_{nn} = 0$ sein, denn sonst wäre $\pi_{hn} = 1$, und die übrigen Einträge der n-ten Zeile von $\bar{\epsilon}$ dürfen maximal eine Eins enthalten, denn sonst hätte π in der h-ten Zeile mehr als eine Eins. Folglich ist $\bar{\delta}$ vom Typ r und $\bar{\epsilon}$ vom Typ p oder r′.

$\underline{\exists h, l < n\,(h \neq l) : \bar{\delta}_{hn} = 1, \bar{\delta}_{ln} = 1}$: Dann darf $\bar{\epsilon}$ in der n-ten Zeile keine Eins enthalten, denn sonst gäbe es in π eine Spalte mit zwei Einsen. Also ist $\bar{\epsilon}$ vom Typ p.

In jedem Fall ist eine der beiden Matrizen $\bar{\delta}$ oder $\bar{\epsilon}$ vom Typ p oder $\bar{\delta}$ ist vom Typ r und $\bar{\epsilon}$ vom Typ r′. Da $\bar{\delta} \cong \delta$ und $\bar{\gamma} \cong \gamma$ gilt, ist die Aussage des Lemmas für π damit bewiesen.
Sei nun $\alpha \in \mathbf{B}_n$ vom Typ p und $\beta, \gamma \in \mathbf{B}_n$ mit $\alpha = \beta\gamma$. Dann existieren nach Lemma 2.5 auf Seite 16 Permutationen $\mu, \nu \in \mathbf{S}_n$ mit $\pi = \mu\alpha\nu = (\mu\beta)(\gamma\nu)$. Wie eben gezeigt, gilt die Aussage des Lemmas für $\mu\beta$ und $\gamma\nu$ und wegen $\mu\beta \cong \beta$ und $\gamma\nu \cong \gamma$ auch für β und γ. □

Bemerkung: Wir haben im Beweis bei $\bar{\delta}$ und $\bar{\epsilon}$ schon geschlossen, daß sie vom Typ p sind, obwohl $\tilde{\delta}$ und $\tilde{\epsilon}$ nicht zwangsläufig Einheitsmatrizen sind, wie in der Definition vorgegeben. Durch Permutieren der ersten $n-1$ Zeilen oder Spalten ist dies aber erreichbar und die entsprechenden Matrizen sind jeweils äquivalent und damit vom selben Typ. In den folgenden Beweisen werden wir ebenso verfahren (auch bei Matrizen des Typs t).

2.15 Lemma *Es sei $\alpha \in \mathbf{B}_n$ vom Typ r und $\beta, \gamma \in \mathbf{B}_n$ mit $\alpha = \beta\gamma$. Dann ist eine der beiden Matrizen β oder γ vom Typ p oder vom Typ r.*

Beweis: Analog zum Beweis des vorherigen Lemmas zeigen wir die Aussage für $\varrho = \beta\gamma$, wobei β und γ die in Lemma 2.13 auf Seite 18 gezeigte Gestalt haben:

$$\beta = \begin{pmatrix} \ulcorner & & \urcorner & * \\ & \tilde{\beta} & & \vdots \\ \llcorner & & \lrcorner & * \\ * & \dots & * & * \end{pmatrix}, \quad \gamma = \begin{pmatrix} \ulcorner & & \urcorner & * \\ & \tilde{\gamma} & & \vdots \\ \llcorner & & \lrcorner & * \\ * & \dots & * & * \end{pmatrix} \quad (\tilde{\beta}, \tilde{\gamma} \in \mathbf{S}_{n-1}).$$

Für $i \in \underline{n-1}$ gilt $\beta_{ni} = 0$, denn ansonsten gäbe es in der n-ten Zeile von α einen Eintrag ungleich Null.
Weiterhin existiert genau wie im Beweis zu Lemma 2.13 auf Seite 18 ein $(n-1)$-Tupel $K = (k_1, \dots, k_{n-1})$, so daß für jedes $i \in \underline{n-1}$ gilt: $\beta_{ik_i} = 1 = \gamma_{k_i i}$.
Versuchen wir jetzt, die unbestimmten Einträge von β und γ zu untersuchen, so ergibt sich folgende Fallunterscheidung:

$\underline{\beta_{nn} = 1}$: Dann darf die n-te Zeile von γ keine Eins enthalten, denn sonst hätte ϱ in der n-ten Zeile eine Eins. Des weiteren muß $\gamma_{k_{n-1}n} = 1$ und $\gamma_{kn} = 0$ (für $k \neq k_{n-1}$) sein, denn nur so ist $\varrho_{n-1,n} = 1$ und $\varrho_{ln} = 0$ für $l \neq n-1$. Damit ist γ vom Typ r.

$\underline{\beta_{nn} = 0}$: Dann ergibt sich weiter:

$\underline{\gamma_{nn} = 1}$: Nun ist noch die letzte Spalte von β zu betrachten:

$\underline{\beta_{*n} = \mathbf{0}}$: Dann ist β vom Typ p.

$\underline{\beta_{*n} \neq \mathbf{0}}$: Dann darf höchstens der Eintrag $\beta_{n-1,n} = 1$ sein, denn jede andere Eins in der n-ten Spalte von β würde wegen $\gamma_{nn} = 1$ die n-te Spalte von ϱ nicht korrekt erzeugen. Also ist β vom Typ r.

$\underline{\gamma_{nn} = 0}$: um die n-te Spalte von ϱ erzeugen zu können, muß $\gamma_{k_{n-1}n} = 1$ und $\gamma_{kn} = 0$ für $k \neq k_{n-1}$ gelten. Für die letzte Spalte von β ergibt sich damit:

$\underline{\beta_{*n} = \mathbf{0}}$: Dann ist β vom Typ p.

$\underline{\exists! k < n : \beta_{kn} = 1}$: Dann ist β vom Typ r.

$\underline{\exists k, l < n (k \neq l) : \beta_{kn} = 1, \beta_{ln} = 1}$: Dann muß $\gamma_{n*} = \mathbf{0}$ sein, denn sonst gäbe es zwei Einsen in einer Spalte von ϱ. Folglich ist γ vom Typ r.

In jedem der sechs Fälle ist eine der beiden Matrizen β und γ vom Typ p oder vom Typ r und es ist keine andere Belegung der letzten Spalte und Zeile von β und γ möglich, wenn $\beta\gamma = \varrho$ gelten soll. In Abbildung A auf der nächsten Seite ist die Fallunterscheidung für das Produkt $\beta\gamma$ in Form eines Baumes dargestellt.
Schließlich existieren für die Typ r Matrix $\alpha = \delta\epsilon$ Permutationen μ und ν, so daß $\varrho = \mu\alpha\nu = (\mu\delta)(\epsilon\nu)$ gilt. Damit folgt wegen $\mu\delta \cong \delta$ und $\epsilon\nu \cong \epsilon$ die Aussage des Lemmas auch für δ und ϵ. □
Analog zum Beweis des obigen Lemmas läßt sich zeigen:

2.16 Lemma *Wenn $\alpha \in \mathbf{B}_n$ vom Typ r′ ist und β, γ existieren mit $\alpha = \beta\gamma$, dann ist eine der beiden Matrizen β oder γ vom Typ p oder vom Typ r′.*

2.17 Lemma *Wenn $\alpha \in \mathbf{B}_n$ vom Typ t ist und β, γ existieren mit $\alpha = \beta\gamma$, dann ist eine der beiden Matrizen β oder γ vom Typ t.*

Beweis: Auch dieser Beweis folgt dem Schema der Beweise in Lemma 2.14 auf Seite 20 und 2.15 auf der vorherigen Seite und daher zeigen wir hier nur die Aussage für $\tau = \beta\gamma$. Dabei haben β und γ die in Lemma 2.13 auf Seite 18 gezeigte Gestalt und es existiert ein $(n-1)$-Tupel $K = (k_1, \ldots, k_{n-1})$ mit $\beta_{ik_i} = 1 = \gamma_{k_i i}$ für jedes $i \in \underline{n-1}$.
Dann ergeben sich zwingend folgende Belegungen für die letzte Spalte und Zeile von β und γ:

- Für jedes $j \in \underline{n-1}$ muß $\beta_{nj} = 0$ sein, denn würde ein $k \in \underline{n-1}$ existieren mit $\beta_{nk} = 1$, so gäbe es ein $i \in \underline{n-1}$ mit $k_i = k$ und damit wäre $\tau_{ni} = 1$.
- Dann muß $\beta_{nn} = 1$ und $\gamma_{nn} = 1$ gelten, denn sonst wäre $\tau_{nn} = 0$.
- Für jedes $j \in \underline{n-1}$ muß $\gamma_{nj} = 0$ sein, denn würde ein $k \in \underline{n-1}$ existieren mit $\gamma_{nk} = 1$, so wäre wegen $\beta_{nn} = 1$ auch $\tau_{nk} = 1$.
- Für jedes $j \in \underline{n-2}$ muß $\beta_{jn} = 0$ sein, denn würde ein $k \in \underline{n-2}$ existieren mit $\beta_{kn} = 1$, so wäre wegen $\gamma_{nn} = 1$ auch $\tau_{kn} = 1$.

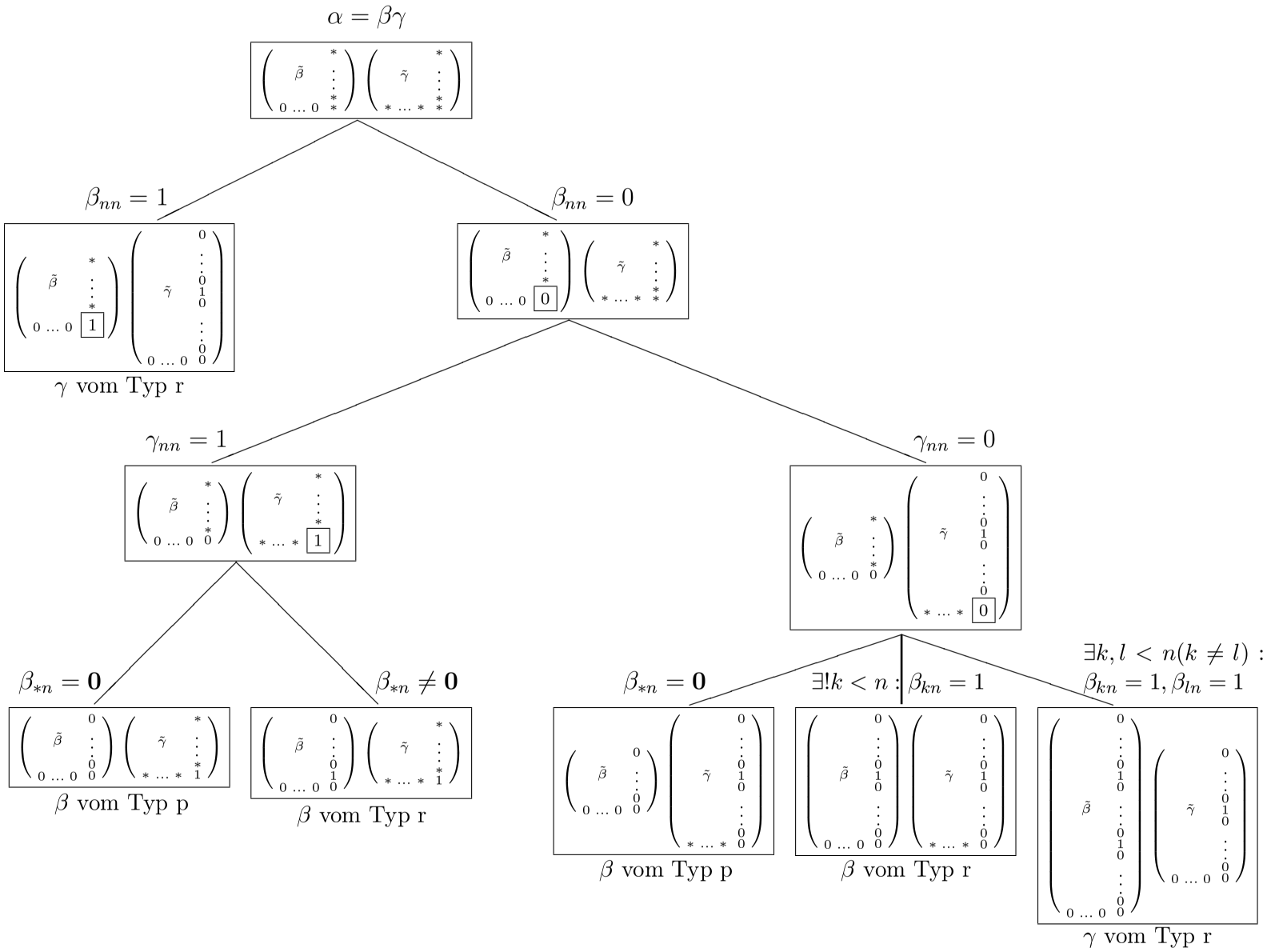


Abbildung 3: Übersicht zur Fallunterscheidung beim Beweis zu Lemma 2.15

- Für jedes $j \in \underline{n-1}$ mit $j \neq k_{n-1}$ muß $\gamma_{jn} = 0$ gelten, denn würde ein $k \in \underline{n-1}$ $(k \neq k_{n-1})$ existieren mit $\gamma_{kn} = 1$, so gäbe es eine Zeile $i \in \underline{n-2}$ mit $\beta_{ik} = 1$ und damit wäre $\tau_{in} = 1$.

Es ergibt sich also, daß β und γ folgendermaßen aussehen müssen:

$$\beta = \begin{array}{c} \\ 1 \\ \\ n-1 \\ n \end{array} \begin{pmatrix} \ulcorner & & \urcorner & 0 \\ & \tilde{\beta} & & \vdots \\ & & & 0 \\ \llcorner & & \lrcorner & * \\ 0 & \dots & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{array}{c} 1 \\ \\ k_{n-1} \\ \\ \\ n \end{array} \begin{pmatrix} \ulcorner & & \urcorner & 0 \\ & & & \vdots \\ & & & 0 \\ & \tilde{\gamma} & & * \\ & & & 0 \\ & & & \vdots \\ \llcorner & & \lrcorner & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}, \quad (\tilde{\beta}, \tilde{\gamma} \in \mathbf{S}_{n-1})$$

Ist der Eintrag $\beta_{n-1,n}$ gleich Eins, dann ist β vom Typ t. Wenn der Eintrag $\beta_{n-1,n}$ gleich Null ist, so muß $\gamma_{k_{n-1}n} = 1$ gelten, denn sonst wäre $\alpha_{n-1,n}$ gleich Null. Dann ist γ vom Typ t. □

B. Reguläre Matrizen

Der Begriff der Regularität wurde durch John von Neumann im Zusammenhang mit Ringen erstmals verwendet [vN36]. In [Kim82] schreibt Ki Hang Kim: „regular elements are of interest because of their close relationship with inverses“. Die folgende Definition ist zwar schon für den Spezialfall der Booleschen Matrizen aufbereitet, unterscheidet sich aber inhaltlich nicht vom allgemeinen Fall einer Halbgruppe.

2.18 Definition Ein Element α des Monoids $\mathbf{B}_n$ heißt *regulär*, wenn ein $\beta \in \mathbf{B}_n$ existiert, so daß $\alpha = \alpha\beta\alpha$ gilt.

Demnach sind die Permutationsmatrizen naheliegende Beispiele für Regularität, denn zu jedem $\mu \in \mathbf{S}_n$ operiert $\mu^\top$ als Inverses in $\mathbf{B}_n$ und daher gilt: $\mu = \mu\Delta = \mu(\mu^\top\mu)$.
Nachfolgend geben wir zunächst Kriterien für die Regularität einer Matrix $\alpha \in \mathbf{B}_n$ an. Diese nutzen wir in Abschnitt 3, um ein minimales Erzeugendensystem für das von den regulären Elementen erzeugte Untermonoid $\mathbf{B}_n^r$ zu finden.

2.19 Lemma *Seien $\alpha, \beta \in \mathbf{B}_n$ mit $\alpha \cong \beta$. Dann gilt: α ist genau dann regulär, wenn β regulär ist.*

Beweis: Da α und β äquivalent sind, existieren $\mu, \nu \in \mathbf{S}_n$ mit $\alpha = \mu\beta\nu$ sowie $\beta = \mu^\top\alpha\nu^\top$. Wenn α regulär ist, existiert des weiteren ein γ mit $\alpha = \alpha\gamma\alpha$ und daher gilt:

$$\beta = \mu^\top\alpha\nu^\top = \mu^\top(\alpha\gamma\alpha)\nu^\top = \mu^\top(\mu\beta\nu)\gamma(\mu\beta\nu)\nu^\top = \beta(\mu\gamma\nu)\beta.$$

Demnach ist β ebenfalls regulär. Die umgekehrte Richtung zeigt man analog. □

2.20 Folgerung Wenn $\alpha \in \mathbf{B}_n$ vom Typ t, p, r oder r′ ist, dann ist α regulär. Denn einfaches Nachrechnen zeigt, daß die Matrizen τ, π, ϱ und ϱ' allesamt idempotent (das heißt es gilt $\tau\tau = \tau$, $\pi\pi = \pi$, usw.) und damit auch regulär sind. Weiterhin ist ja nach Lemma 2.5 auf Seite 16 beispielsweise ein α vom Typ t äquivalent zu τ und damit nach dem vorhergehenden Lemma ebenfalls regulär.

In seiner wegweisenden Arbeit „Die Halbgruppe der binären Relationen“ ([Zar63], Theorem 3.2) zeigt Zarecki den Zusammenhang zwischen der Regularität eines Elementes von $\mathbf{B}_n$ und der Distributivität seines Zeilenverbandes:

2.21 Satz ([Zar63]) *Eine Matrix $\alpha \in \mathbf{B}_n$ ist genau dann regulär, wenn der Zeilenverband $\mathfrak{Z}(\alpha)$ vollständig distributiv ist.*

Die Bedeutung dieses Lemmas liegt vor allem darin, daß es einen Zusammenhang zwischen der Regularität einer Matrix als Eigenschaft des Relationenproduktes (im Monoid $\mathbf{B}_n$) und der Distributivität des Zeilenverbandes (einer Ordnungsstruktur) herstellt. Das Lemma wurde auch von Yang [Yan69] bewiesen.
Für praktische Zwecke, um zu testen ob eine Matrix regulär ist, bietet sich ein Kriterium von Boris M. Schein [Sch76] an. Danach ist $\alpha \in \mathbf{B}_n$ genau dann regulär, wenn $\alpha = \alpha(\overline{\alpha^\top \overline{\alpha} \alpha^\top})\alpha$ gilt, wobei $\overline{\alpha}$ die zu α komplementäre Matrix ist, das heißt die Nullen und Einsen sind vertauscht ($\overline{\alpha}_{ij} = 1 \iff \alpha_{ij} = 0$).

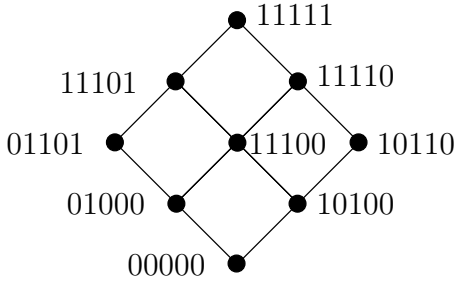


Abbildung 4: Hasse-Diagram für $\mathfrak{Z}(\alpha)$

2.22 Beispiel Sei $\alpha \in \mathbf{B}_n$ folgendermaßen definiert:

$$\alpha := \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Zuerst stellen wir fest, daß α nach dem Kriterium von Schein regulär ist. Es gilt:

$$\alpha = \alpha \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \alpha.$$

Des weiteren ist

$$\mathfrak{Z}(\alpha) = \{(11111), (10110), (01101), (01000), (11110), (10100), (11101), (11100), (00000)\}$$

und es ergibt sich für $\mathfrak{Z}(\alpha)$ das Hasse-Diagramm in Abbildung 4 auf der vorherigen Seite, an welchem man sieht, daß der Zeilenverband distributiv ist.

Basierend auf dem in Satz 2.21 auf der vorherigen Seite festgehaltenen Ergebnis von Zarecki wurde in [KR78] das folgende Kriterium für die Regularität einer Booleschen Matrix bewiesen:

2.23 Lemma ([KR78]) *Eine Matrix $\alpha \in \mathbf{B}_n$ ist genau dann regulär, wenn eine Menge A von Zeilen aus α existiert, so daß A den gesamten Zeilenverband von α aufspannt und für jede Zeile $\alpha_{i*} \in A$ ein Boolescher Vektor u_i existiert, so daß folgendes gilt:*

(1) u_i *ist ein Einheitsvektor*

(2) $u_i \leq \alpha_{i*}$

(3) für alle anderen $\alpha_{j*} \in A$ *gilt:* $u_i \leq \alpha_{j*} \Rightarrow \alpha_{i*} \leq \alpha_{j*}$.

Beweis: Es folgt der Beweis, daß für jede reguläre Matrix eine solche Menge von Zeilen existiert. Die Rückrichtung dieses Lemmas ergibt sich in [KR78] im Beweis zu Theorem 7.2.
Sei $\alpha \in \mathbf{B}_n$ regulär und $A := \mathfrak{Z}_B(\alpha)$. Dann spannt A den ganzen Zeilenverband von α auf. Für $\alpha_{i*} \in A$ sei die Menge C_i wie folgt definiert:

$$C_i := \{\alpha_{j*} \in \mathfrak{Z}_B(\alpha) \mid \alpha_{i*} \not\leq \alpha_{j*}\}.$$

C_i enthält also alle Zeilen der Zeilenbasis von α, die nicht größer oder gleich α_{i*} sind.
Zunächst stellen wir fest, daß die Bedingung (3) für einen Vektor $u_i \in \mathbf{V}_n$, der (1) und (2) erfüllt, äquivalent ist zu

$$u_i \not\leq \bigvee_{\alpha_{j*} \in C_i} \alpha_{j*}. \qquad (\star)$$

Denn wenn (3) gilt und $u_i \leq \bigvee_{\alpha_{j*} \in C_i} \alpha_{j*}$ wäre, dann gäbe es ein $\alpha_{j*} \in C_i$ mit $u_i \leq \alpha_{j*}$ aber $\alpha_{i*} \not\leq \alpha_{j*}$, im Widerspruch zu (3). Wenn andererseits $(\star)$ gilt und es ein $\alpha_{j*} \in A$ gäbe mit $u_i \leq \alpha_{j*}$ und $\alpha_{i*} \not\leq \alpha_{j*}$, dann wäre $\alpha_{j*} \in C_i$ und damit $u_i \not\leq \alpha_{j*}$ im Widerspruch zur Annahme $u_i \leq \alpha_{j*}$.
Daher folgt, daß die Existenz eines u_i, welches (1), (2) und (3) erfüllt, äquivalent ist zu

$$\alpha_{i*} \not\leq \bigvee_{\alpha_{j*} \in C_i} \alpha_{j*}. \qquad (\star\star)$$

Denn das u_i „markiert“ ja gerade jene Stelle in α_{i*}, an der α_{i*} größer als alle α_{j*} aus C_i ist.
Angenommen, $(\star\star)$ gilt nicht, d.h. $\alpha_{i*} \leq \bigvee_{\alpha_{j*} \in C_i} \alpha_{j*}$. Dann betrachten wir die Ungleichung im Zeilenverband von α und können auf beiden Seiten das Infimum mit α_{i*} bilden:

$$\alpha_{i*} \wedge \alpha_{i*} \leq \left(\bigvee_{\alpha_{j*} \in C_i} \alpha_{j*} \right) \wedge \alpha_{i*}.$$

Bemerkung: das Infimum in $\mathfrak{Z}(\alpha)$ entspricht im allgemeinen *nicht* dem Infimum in $\mathbf{V}_n$. Wegen der Idempotenz von $\wedge$ und der Äquivalenz von $a \leq b$ und $a = b \wedge a$ in einem Verband gilt sogar:

$$\alpha_{i*} = \left(\bigvee_{\alpha_{j*} \in C_i} \alpha_{j*} \right) \wedge \alpha_{i*}.$$

Da α regulär ist, ist der Zeilenverband von α nach Satz 2.21 auf Seite 25 distributiv und damit folgt:

$$\alpha_{i*} = \bigvee_{\alpha_{j*} \in C_i} (\alpha_{j*} \wedge \alpha_{i*}).$$

Weil die $\alpha_{j*} \in C_i$ alle nicht größer oder gleich α_{i*} sind, ist $\alpha_{j*} \wedge \alpha_{i*}$ stets echt kleiner als α_{i*}. Damit ist α_{i*} Supremum von echt kleineren Elementen der Zeilenbasis und kann daher selbst kein Element der Zeilenbasis sein. Dies widerspricht der Voraussetzung $\alpha_{i*} \in A$ und daher muß die Annahme, daß $(\star\star)$ nicht gilt, falsch sein. Folglich existiert ein u_i, welches die Bedingungen (1), (2) und (3) erfüllt. □

2.24 Beispiel Wir betrachten die in Beispiel 2.22 definierte reguläre Matrix α. Für α ist $A = \{\alpha_{1*}, \alpha_{2*}, \alpha_{3*}, \alpha_{5*}\}$ mit den Einheitsvektoren $u_1 = (00010)$, $u_2 = (00001)$, $u_3 = (01000)$ und $u_5 = (10000)$ eine Menge entsprechend dem Lemma.

C. Prime Matrizen

Bei der Betrachtung eines Erzeugendensystems für $\mathbf{B}_n$ spielen *prime Matrizen* eine wesentliche Rolle, denn diese lassen sich (bis auf Äquivalenz) nicht in Faktoren zerlegen. Prime Boolesche Matrizen wurden von de Caen und Gregory in [dCG80] und [dCG81] untersucht. Die dort gezeigten hinreichenden Bedingungen für prime Matrizen benutzen wir, um zu zeigen, daß die Anzahl der primen Matrizen exponentiell in n wächst.

2.25 Definition Ein $\alpha \in \mathbf{B}_n \setminus \mathbf{S}_n$ heißt *prim*, wenn aus $\alpha = \beta\gamma$ stets $\beta \in \mathbf{S}_n$ oder $\gamma \in \mathbf{S}_n$ folgt.

2.26 Bemerkung In $\mathbf{B}_1$ und $\mathbf{B}_2$ gibt es keine primen Matrizen. Denn in $\mathbf{B}_2$ hat jede Nicht-Permutationsmatrix entweder eine Null-Zeile (-Spalte) oder eine der Zeilen (Spalten) ist in einer anderen Zeile (Spalte) schon enthalten. In beiden Fällen läßt sich die Matrix in ein Produkt aus sich selbst und eine der in 2.8 auf Seite 17 und 2.10 auf Seite 18 definierten Nicht-Permutationsmatrizen zerlegen. In $\mathbf{B}_3$ gibt es genau sechs prime Matrizen.

2.27 Lemma *Sei $\alpha \in \mathbf{B}_n$ prim. Dann ist der Zeilenverband $\mathfrak{Z}(\alpha)$ maximal (das heißt für alle $\beta \in \mathbf{B}_n$ mit $\mathfrak{Z}(\alpha) \subseteq \mathfrak{Z}(\beta)$ gilt $\mathfrak{Z}(\alpha) = \mathfrak{Z}(\beta)$ oder $\mathfrak{Z}(\beta) = \mathbf{V}_n$).*

Beweis: Sei $\alpha \in \mathbf{B}_n$ prim. Wenn es ein $\beta \in \mathbf{B}_n$ mit $\mathfrak{Z}(\alpha) \subseteq \mathfrak{Z}(\beta)$ gibt, dann existiert nach Lemma 1.31 auf Seite 10 ein $\gamma \in \mathbf{B}_n$ mit $\alpha = \gamma\beta$. Weil α prim ist, ist β oder γ eine Permutationsmatrix. Ist $\beta \in \mathbf{S}_n$, so gilt $\mathfrak{Z}(\beta) = \mathbf{V}_n$. Ist $\gamma \in \mathbf{S}_n$, dann gilt

$\mathfrak{Z}(\beta) = \mathfrak{Z}(\gamma\beta) = \mathfrak{Z}(\alpha)$, denn γ permutiert ja nur die Zeilen von β und dadurch ändert sich der Zeilenverband nicht. Der Zeilenverband von α ist also maximal. □

2.28 Lemma *Sei $\alpha \in \mathbf{B}_n$ prim. Dann gilt für alle $\beta, \gamma \in \mathbf{B}_n$:*

(1) $\alpha \cong \beta \quad \Rightarrow \quad \beta$ *ist prim*

(2) $\alpha \cong \beta \quad \Longleftrightarrow \quad \alpha \mathscr{D} \beta$

(3) $\alpha = \beta\gamma \quad \Rightarrow \quad \alpha \cong \beta$ *oder* $\alpha \cong \gamma$

Beweis:

(1) Seien α und β äquivalent. Dann existieren $\mu, \nu \in \mathbf{S}_n$ mit $\alpha = \mu\beta\nu$. Angenommen, β ist nicht prim, d.h. es existieren $\beta_1, \beta_2 \in \mathbf{B}_n \setminus \mathbf{S}_n$ mit $\beta = \beta_1\beta_2$. Folglich gilt $\alpha = \mu(\beta_1\beta_2)\nu = (\mu\beta_1)(\beta_2\nu)$, wobei $\mu\beta_1$ und $\beta_2\nu$ nach Lemma 1.32 auf Seite 13 keine Permutationen sind. Damit ist α nicht prim im Widerspruch zur Voraussetzung und deshalb muß β prim sein.

(2) Es gelte $\alpha \mathscr{D} \beta$. Dann folgt aus der Definition der Relation $\mathscr{D}$:

$$\exists \mu, \nu \in \mathbf{B}_n : \alpha = \mu\beta\nu \quad \text{und} \quad \exists \hat{\mu}, \hat{\nu} \in \mathbf{B}_n : \beta = \hat{\mu}\alpha\hat{\nu}$$

Um zu zeigen, daß $\alpha \cong \beta$ gilt, nehmen wir an, daß μ keine Permutationsmatrix ist. Weil α prim ist, gilt dann $\beta\nu \in \mathbf{S}_n$ und nach Lemma 1.32 auf Seite 13 auch $\beta \in \mathbf{S}_n$. Wegen $\beta = \hat{\mu}\alpha\hat{\nu}$ folgt dann ebenso $\hat{\mu}, \alpha, \hat{\nu} \in \mathbf{S}_n$, was der Voraussetzung, daß α prim ist, widerspricht. Daher muß μ eine Permutationsmatrix sein (für ν zeigt man dies analog) und somit gilt $\alpha \cong \beta$.

Es gelte $\alpha \cong \beta$. Dann existieren $\mu, \nu \in \mathbf{S}_n$ mit $\alpha = \mu\beta\nu$ und damit gilt $\mathbf{B}_n\alpha\mathbf{B}_n = \mathbf{B}_n\mu\beta\nu\mathbf{B}_n \subseteq \mathbf{B}_n\beta\mathbf{B}_n$.
Ebenso gilt $\beta = \mu^\top\alpha\nu^\top$ und folglich $\mathbf{B}_n\beta\mathbf{B}_n = \mathbf{B}_n\mu^\top\alpha\nu^\top\mathbf{B}_n \subseteq \mathbf{B}_n\alpha\mathbf{B}_n$.

(3) Sei $\alpha = \beta\gamma$, dann muß eine der beiden Matrizen β oder γ eine Permutation sein. Sei dies o.B.d.A. β. Dann gilt $\alpha = \beta\gamma\Delta$ mit $\beta, \Delta \in \mathbf{S}_n$ und daher $\alpha \cong \gamma$. Analog folgt aus $\gamma \in \mathbf{S}_n$ gerade: $\alpha \cong \beta$. □

2.29 Folgerung Ist eine Matrix in einer Äquivalenzklasse von $\mathscr{D}$ prim, so sind alle Matrizen dieser Äquivalenzklasse prim. Es ist daher legitim diese Klassen, die eine prime Matrix enthalten, im weiteren Verlauf als *prime $\mathscr{D}$-Klassen* zu bezeichnen.

2.30 Definition Sei $\alpha \in \mathbf{B}_n$, $\{z_1, \ldots, z_k\} \subseteq \underline{n}$ und $\{s_1, \ldots, s_l\} \subseteq \underline{n}$. Dann heißt $\beta = (\beta_{ij})_{\substack{i=1,\ldots,k \\ j=1,\ldots,l}}$ *Teilmatrix von* α, falls $(\beta_{ij}) = (\alpha_{z_i s_j})$ für alle $i = 1, \ldots, k$ und $j = 1, \ldots, l$ gilt.

2.31 Definition Eine Matrix $\alpha \in \mathbf{B}_n$ heißt *voll-unzerlegbar*, wenn α keine Nullmatrix der Größe $k \times (n-k)$ (mit $0 < k < n$) als Teilmatrix hat.

Wie wir später (in Lemma 2.37 auf Seite 31) sehen werden, haben prime Matrizen stets maximalen Zeilen- und Spaltenrang. Die einzigen (bis auf Äquivalenz) voll-unzerlegbaren Matrizen in $\mathbf{B}_4$ mit dieser Eigenschaft sind:

$$\alpha_1 := \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad \alpha_2 := \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad \alpha_3 := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

2.32 Definition Sei $\alpha \in \mathbf{B}_n$. Wir betrachten alle (2×2)-Teilmatrizen von α, die nur aus Einsen bestehen und ersetzen in α alle Einsen, die in solchen (2×2)-Teilmatrizen liegen, durch Nullen. Die entstehende Matrix wird mit $\alpha^{\square}$ bezeichnet.

In der nebenstehenden Matrix sind Einsen, die zu einer (2×2)-Teilmatrix gehören, fett gedruckt dargestellt. Für die Matrizen aus dem vorhergehenden Beispiel ergibt sich:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ \mathbf{1} & 0 & \mathbf{1} & 1 \\ 1 & 1 & 0 & 1 \\ \mathbf{1} & 1 & \mathbf{1} & 0 \end{pmatrix}$$

$$\alpha_1^{\square} = \mathbf{0}, \quad \alpha_2^{\square} = \alpha_2, \quad \alpha_3^{\square} = \alpha_3.$$

Das folgende Lemma werden wir nutzen, um eine untere Schranke für die Anzahl primer Matrizen zu finden. Es folgt als Korollar 3.4 direkt aus Theorem 3.3, welches in [dCG81] bewiesen wird.

2.33 Lemma ([dCG81]) *Sei $\alpha \in \mathbf{B}_n$. Wenn α voll-unzerlegbar ist und ein $\mu \in \mathbf{S}_n$ existiert mit $\mu \leq \alpha^{\square}$, dann ist α prim.*

Folglich sind α_2 und α_3, aber nicht α_1 prim, denn es gilt:

$$\alpha_2^{\square} = \alpha_2 \leq \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathbf{S}_n \quad \text{und} \quad \alpha_3^{\square} = \alpha_3 \leq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathbf{S}_n.$$

Der folgende Satz ist [Kim82] (Theorem 2.4.1) entnommen und der Beweis dort unvollständig bzw. falsch abgedruckt worden. Daher folgt hier ein ausführlicher Beweis.

2.34 Satz *In $\mathbf{B}_n$ gibt es mindestens $2^{\frac{n^2}{4}-\mathcal{O}(n)}$ prime Matrizen.*

Beweis: Wir betrachten die Menge $\hat{\mathbf{P}}_n \subseteq \mathbf{B}_n$ aller Matrizen $\alpha = (\alpha_{ij})_{i,j \in \underline{n}}$ der folgenden Form:

$$\begin{aligned} i = j \text{ oder } i = j+1 \text{ oder } (i,j) = (1,n) \quad &\Rightarrow \quad \alpha_{ij} = 1 && (1) \\ (j > i \text{ und } (i,j) \neq (1,n)) \text{ oder } (i,j) = (n,1) \quad &\Rightarrow \quad \alpha_{ij} = 0 && (2) \\ i > j \text{ und } 0 \equiv i - j \bmod 2 \quad &\Rightarrow \quad \alpha_{ij} = 0 && (3) \\ i > j+1 \text{ und } 1 \equiv i - j \bmod 2 \text{ und } (i,j) \neq (n,1) \quad &\Rightarrow \quad \alpha_{ij} \in \{0,1\} && (4) \end{aligned}$$

Durch Regel (4) dürfen gewisse Diagonalen dieser Matrizen frei belegt werden.
Die folgende Matrix zeigt die Struktur für $n = 8$. Dabei können die Einträge in denen ein $*$ steht beliebig mit 0 oder 1 belegt werden:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ * & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & * & 0 & 1 & 1 & 0 & 0 & 0 \\ * & 0 & * & 0 & 1 & 1 & 0 & 0 \\ 0 & * & 0 & * & 0 & 1 & 1 & 0 \\ 0 & 0 & * & 0 & * & 0 & 1 & 1 \end{pmatrix}$$

Unabhängig von der Belegung der $*$-Einträge gilt für alle Matrizen in $\hat{\mathbf{P}}_n$:

(a) Sie sind voll-unzerlegbar, da sie keine $k \times (n-k)$ Nullmatrix als Teilmatrix haben (mit $0 < k < n$). Der „worst-case“ wäre eine Belegung aller Einträge aus (4) mit Nullen. Weil aber die untere Nebendiagonale nur Einsen enthält und $\alpha_{1n} = 1$ ist, existiert keine Nullmatrix dieser Größe als Teilmatrix.

(b) Keine Eins der Hauptdiagonale liegt in einer 2×2 Teilmatrix, die aus lauter Einsen besteht. Auch im Fall der Belegung aller Einträge aus (4) mit Einsen gilt dies noch.

Aus (b) folgt für alle $\alpha \in \hat{\mathbf{P}}_n$, daß $\Delta \leq \alpha^{\square}$ gilt. Denn alle Einsen auf der Hauptdiagonale bleiben in $\alpha^{\square}$ erhalten. Folglich können wir Lemma 2.33 auf der vorherigen Seite anwenden und damit sind alle Matrizen der Menge $\hat{\mathbf{P}}_n$ prim.
Wollen wir die Anzahl der Elemente in $\hat{\mathbf{P}}_n$ bestimmen, so müssen wir die Anzahl der frei belegbaren Einträge zählen. Für $n = 3$ und $n = 4$ ergibt sich jeweils genau eine Matrix. Für $n > 4$ sind jeweils $\left\lfloor \frac{n-3}{2} \right\rfloor$ Nebendiagonalen frei belegbar und „im Mittel“ enthält jede dieser Diagonalen $\left\lfloor \frac{n}{2} \right\rfloor$ Elemente – dies ist sogar der exakte Mittelwert. Dadurch ergibt sich für die Anzahl der frei wählbaren Einträge:

$$\begin{aligned} \left\lfloor \frac{n-3}{2} \right\rfloor \left\lfloor \frac{n}{2} \right\rfloor &\geq \left(\frac{n-4}{2} \right) \left(\frac{n-1}{2} \right) \\ &= \frac{n^2 - 5n + 4}{4} \\ &= \frac{n^2}{4} - \frac{5n-4}{4} \\ &= \frac{n^2}{4} - \mathcal{O}(n) \end{aligned}$$

Damit gilt $|\hat{\mathbf{P}}_n| \geq 2^{\frac{n^2}{4} - \mathcal{O}(n)}$ und alle Matrizen in $\hat{\mathbf{P}}_n$ sind prim. Die Anzahl der primen Matrizen wächst also exponentiell in n. $\square$

2.35 Bemerkung Noch zu beweisen ist, daß keine zwei Matrizen in $\hat{\mathbf{P}}_n$ existieren, die zueinander äquivalent sind. Denn dann wäre gezeigt, daß auch die Anzahl primer $\mathscr{D}$-Klassen exponentiell in n wächst.
Es ist leicht zu sehen, daß es mindestens $\left\lfloor \frac{n-3}{2} \right\rfloor \left\lfloor \frac{n}{2} \right\rfloor$ prime $\mathscr{D}$-Klassen geben muß, denn zwei Matrizen mit unterschiedlich vielen Einsen können nicht äquivalent zueinander sein. In $\mathbf{B}_3$ gibt es genau eine prime $\mathscr{D}$-Klasse, in $\mathbf{B}_4$ sind es drei und in $\mathbf{B}_5$ sogar neun $\mathscr{D}$-Klassen primer Matrizen.
In [Kon02] schreibt Konieczny: „the number of prime $\mathscr{D}$-classes in $\mathbf{B}_n$ grows at least exponentially with n“ und verweist auf den in [Kim82] (Theorem 2.4.1) abgedruckten und hier zitierten Satz 2.34. Aus diesem ist jedoch nicht offensichtlich, daß die definierten Matrizen paarweise nicht äquivalent sind. Als Quelle gibt Kim einen Seminar-Report [DKR76] aus dem Jahre 1976 an. In ihrer Arbeit [KR77] aus dem Jahre 1977 verweisen Kim und Roush jedoch auf Devadze [Dev68]: „Devadze obtained results, which show, that the growth of the size of minimal generating sets for $\mathbf{B}_n$ is at least exponential.“ In Devadzes Arbeit, die Grundlage des in Abschnitt 4 gezeigten Satzes ist, wird jedoch nur ein lineares Wachstum gezeigt.
Zusammenfassend ist zu sagen, daß nach der Meinung der einschlägigen Autoren die Anzahl der primen $\mathscr{D}$-Klassen exponentiell in n wächst. Ein Beweis hierfür konnte von mir jedoch nicht gefunden werden.

D. Magere Matrizen

In seinem Artikel „A Proof of Devadze's Theorem on Generators of the Semigroup of Boolean Matrices“ [Kon05] führt Konieczny den Begriff „trim“ für eine spezielle Klasse von Booleschen Matrizen ein. Im Deutschen haben wir diese Matrizen „mager“ getauft – der Dank für diesen Vorschlag gebührt Joachim Hereth-Correira.
Die Betrachtung magerer Matrizen ist ein wesentlicher Schritt zum Beweis des Theorems von Devadze, denn zu jeder Booleschen Matrix kann man eine magere Matrix „konstruieren“ und braucht dann lediglich ein Erzeugendensystem für die mageren Matrizen angeben.

2.36 Definition Eine Matrix $\alpha \in \mathbf{B}_n$ heißt *mager*, wenn jede Zeile und jede Spalte von α minimal ist (vgl. Definition 1.29 auf Seite 10).

Ein einfaches Beispiel für magere Matrizen sind die Permutationen, denn keine der Zeilen einer Permutationsmatrix ist in einer anderen Zeile enthalten – gleiches gilt für die Spalten.

2.37 Lemma *Jede prime Matrix ist mager und hat maximalen Zeilen- und Spaltenrang.*

Beweis: Sei $\alpha \in \mathbf{B}_n$ prim. Angenommen, es existiert eine Zeile α_{i*}, welche nicht minimal ist. Dann gibt es eine weitere Zeile $\alpha_{j*}\,(\alpha_{j*} \neq \mathbf{0})$, für die $\alpha_{j*} \leq \alpha_{i*}$ gilt. Nach den Rechenregeln im Zeilenverband gilt dann auch $\alpha_{i*} = \alpha_{i*} \vee \alpha_{j*}$ und daher $\alpha = T^{ij}\alpha$, wobei T^{ij} eine Typ t Matrix nach Bemerkung 2.9 auf Seite 17 ist. Da weder α noch T^{ij}

eine Permutation ist, widerspricht dies der Voraussetzung, daß α prim ist. Somit ist jede Zeile von α minimal.
Angenommen, es gibt eine Zeile α_{i*}, die gleich dem Nullvektor ist. Dann würde $\alpha = P^i\alpha$ gelten (siehe Bemerkung 2.11 auf Seite 18) und α wäre nicht prim. Daher hat α keine Nullzeile.
Weil also jede Zeile von α minimal und ungleich dem Nullvektor ist, ist nach Bemerkung 1.30 auf Seite 10 auch jede Zeile von α in der Zeilenbasis enthalten und damit ist der Zeilenrang maximal.
Analog zeigt man, daß jede Spalte minimal und ungleich $\mathbf{0}$ und der Spaltenrang maximal ist. Die Matrix α ist damit mager mit maximalem Zeilen- und Spaltenrang. □

3. Erzeugendensysteme für Untermonoide von $\mathbf{B}_n$

Wenn wir eine Teilmenge von $\mathbf{B}_n$ betrachten und die Einheitsmatrix sowie alle möglichen Produkte der Elemente der Menge hinzufügen, dann erhalten wir das *Erzeugnis* der Teilmenge. Da es durch Hinzufügen der Produkte abgeschlossen ist bezüglich der Matrizenmultiplikation und die Einheitsmatrix enthält, ist es ein Untermonoid von $\mathbf{B}_n$. In diesem Kapitel werden wir Mengen betrachten, die ganz bestimmte Untermonoide erzeugen und damit die Grundlagen für den Beweis des Theorems von Devadze im nächsten Kapitel legen.

3.1 Definition Sei $A \subseteq \mathbf{B}_n$. Das kleinste Untermonoid von $\mathbf{B}_n$, welches A enthält, nennt man das *von A erzeugte Untermonoid* und bezeichnet es mit $\langle A\rangle$.

3.2 Definition Sei $A \subseteq \mathbf{B}_n$ ein Untermonoid von $\mathbf{B}_n$ und $E \subseteq \mathbf{B}_n$. Dann heißt E *Erzeugendensystem für A*, falls $\langle E\rangle = A$ gilt.

3.3 Definition Sei $A \subseteq \mathbf{B}_n$ eine Untermonoid von $\mathbf{B}_n$ und $E \subseteq \mathbf{B}_n$ ein Erzeugendensystem für A. Dann heißt E *minimal*, falls für jedes $E' \subseteq E$ mit $\langle E'\rangle = A$ gilt: $E' = E$.

Wenn wir zeigen wollen, daß ein Erzeugendensystem minimal ist, nehmen wir an, daß bereits eine echte Teilmenge ein Erzeugendensystem ist und führen dies zum Widerspruch. Dazu zeigen wir, daß jedes Element im Erzeugendensystem auch wirklich benötigt wird. Dieses Lemma wird uns dabei in nachfolgenden Beweisen eine Hilfe sein:

3.4 Lemma *Die Mengen $\mathcal{T}, \mathcal{P}, \mathcal{R}, \mathcal{R}', \mathbf{S}_n$ und $\{\alpha \in \mathbf{B}_n \mid \alpha$ ist prim $\}$ sind paarweise disjunkt.*

Beweis: Da für nichtleere Mengen A und B stets

$$A \cap B = \emptyset \quad \Longleftrightarrow \quad a \in A \Rightarrow a \notin B \quad \Longleftrightarrow \quad b \in B \Rightarrow b \notin A$$

gilt, reicht es, wenn wir für jede der obigen Mengen zeigen, daß keines ihrer Elemente in einer der anderen Mengen enthalten ist.

Die Matrizen vom Typ t bzw. p enthalten mehr bzw. weniger als n Einsen und sind deshalb keine Permutationen. Ebenso enthalten alle Matrizen in $\mathcal{R}$ und $\mathcal{R}'$ eine Nullzeile bzw. -spalte und sind daher keine Permutationen.
Die Matrizen vom Typ t enthalten jeweils eine Zeile, die in einer anderen enthalten und damit nicht minimal ist, also sind sie nicht mager. Matrizen des Typs p, r und r′ enthalten jeweils eine Nullzeile oder -spalte und haben damit nicht maximalen Zeilen- und Spaltenrang. Folglich sind nach Lemma 2.37 auf Seite 31 Matrizen des Typs t, p, r und r′ nicht prim. Permutationen sind per Definition nicht prim.
Eine Matrix von einem Typ kann nicht gleichzeitig von einem anderen Typ sein, das ergibt sich direkt aus der Definition. □

3.5 Lemma *Seien $A, E \subseteq \mathbf{B}_n$ mit $A \subseteq \langle E \rangle$. Wenn für alle $\alpha \in A$ stets gilt:*

$$\alpha = \beta\gamma \quad \Rightarrow \quad \beta \in A \text{ oder } \gamma \in A,$$

dann folgt: $A \cap E \neq \emptyset$.

Beweis: Angenommen, $A \cap E = \emptyset$. Sei m folgendermaßen definiert:

$$m := \min\{k \mid \epsilon_1 \cdot \epsilon_2 \cdot \ldots \cdot \epsilon_k = \alpha,\ \alpha \in A,\ \epsilon_i \in E\,(i = 1, \ldots, k)\}.$$

Da E ganz A erzeugt, gibt es für jedes Element aus A mindestens eine solche Darstellung als Produkt von Elementen aus E und wegen $A \cap E = \emptyset$ gilt $m \geq 2$. Sei $\alpha \in \mathbf{B}_n$ so gewählt, daß $\epsilon_i \in E\,(i = 1, \ldots, m)$ existieren mit $\alpha = \epsilon_1 \cdot \epsilon_2 \cdot \ldots \cdot \epsilon_m$. Dann ist weder ϵ_1 noch $\epsilon_2 \cdot \ldots \cdot \epsilon_m$ ein Element von A, denn sonst wäre m nicht minimal. Dies steht aber im Widerspruch zur Voraussetzung, nach der stets einer der Faktoren von α ein Element von A sein muß. Folglich ist die Annahme $A \cap E = \emptyset$ falsch und E enthält mindestens ein Element der Menge A. □

3.6 Folgerung Sei für ein primes $\alpha \in \mathbf{B}_n$ dessen $\mathscr{D}$-Klasse mit D_α bezeichnet. Dann gilt nach Punkt (3) von Lemma 2.28 auf Seite 28 für alle $\beta, \gamma \in \mathbf{B}_n$ mit $\alpha = \beta\gamma$, daß β oder γ in D_α ist. Folglich muß jedes Erzeugendensystem für $\mathbf{B}_n$ mindestens eine Matrix aus D_α, ja sogar eine Matrix aus jeder primen $\mathscr{D}$-Klasse, enthalten.
Ebenso folgt zusammen mit Lemma 2.17 auf Seite 22, daß jedes Erzeugendensystem für $\mathbf{B}_n$ eine Matrix vom Typ t enthalten muß.

Das vorhergehende Lemma ist nützlich, um für bestimmte Mengen von Matrizen zu zeigen, daß ein Erzeugendensystem für $\mathbf{B}_n$ Matrizen der jeweiligen Art enthalten muß. Darauf aufbauend wurden die Lemmata 2.14, 2.15, 2.16 und 2.17 auf den Seiten 20 bis 22 geschrieben. Schaut man sich diese an, so ahnt man schon, daß für Matrizen des Typs p, r oder r′ die Angelegenheit nicht so einfach ist, denn sie lassen sich auch als Produkt von Matrizen eines anderen Typs darstellen. Folglich müssen wir diese drei Typen gesondert behandeln:

3.7 Lemma *Jedes Erzeugendensystem für $\mathbf{B}_n$ enthält eine Matrix vom Typ p oder eine Matrix vom Typ r und eine Matrix vom Typ r′. Genauer:*

$$E \subseteq \mathbf{B}_n \text{ und } \langle E \rangle = \mathbf{B}_n \quad \Rightarrow \quad E \cap \mathcal{P} \neq \emptyset \text{ oder } (E \cap \mathcal{R} \neq \emptyset \text{ und } E \cap \mathcal{R}' \neq \emptyset)$$

Beweis: Sei $E \subseteq \mathbf{B}_n$ ein Erzeugendensystem für $\mathbf{B}_n$ und angenommen es gilt:

$$E \cap \mathcal{P} = \emptyset \text{ und } (E \cap \mathcal{R} = \emptyset \text{ oder } E \cap \mathcal{R}' = \emptyset).$$

Dann sei m wie folgt definiert:

$$m := \min\{k \mid \epsilon_1 \cdot \ldots \cdot \epsilon_k = \alpha,\, \alpha \in \mathcal{P},\, \epsilon_i \in E\,(i = 1, \ldots, k)\}$$

und $\alpha \in \mathcal{P}$ so gewählt, daß $\epsilon_1, \ldots, \epsilon_m \in E$ existieren mit $\alpha = \epsilon_1 \cdot \ldots \cdot \epsilon_m$.
Dann folgt $\epsilon_1 \notin \mathcal{P}$ und $(\epsilon_2 \cdot \ldots \cdot \epsilon_m) \notin \mathcal{P}$, denn ansonsten wäre m nicht minimal. Demnach gilt nach Lemma 2.14 auf Seite 20, daß ϵ_1 vom Typ r und $(\epsilon_2 \cdot \ldots \cdot \epsilon_m)$ vom Typ r′ ist. Da wegen der Minimalität von m auch ϵ_2 und $(\epsilon_3 \cdot \ldots \cdot \epsilon_m)$ nicht vom Typ p sind, folgt nach Lemma 2.16 auf Seite 22, daß ϵ_2 oder $(\epsilon_3 \cdot \ldots \cdot \epsilon_m)$ vom Typ r′ ist. Per Induktion folgt, daß ein ϵ_i mit $i \in \{2, \ldots, m\}$ existieren muß, welches vom Typ r′ ist. Also gilt: $\epsilon_1 \in \mathcal{R}$ und $\epsilon_i \in \mathcal{R}'$, im Widerspruch zur Annahme, daß $E \cap \mathcal{R} = \emptyset$ oder $E \cap \mathcal{R}' = \emptyset$ ist. Demnach ist die Annahme falsch und die Aussage des Lemmas bewiesen. □

A. Das Monoid $\mathbf{S}_n$ aller Permutationen

3.8 Lemma *Für $\mathbf{S}_n$ mit $n \geq 3$ existiert ein Erzeugendensystem mit zwei Elementen, aber keines mit nur einem Element.*

Beweis: Zunächst geben wir ein Erzeugendensystem mit zwei Elementen an. Dabei verwenden wir die Zyklenschreibweise für Permutationen und meinen beim Produkt $(x_1 \ldots x_k)(y_1 \ldots y_l)$, daß zuerst $(x_1 \ldots x_k)$ und dann $(y_1 \ldots y_l)$ angewendet wird.
Die Menge $\{(12\ldots n), (12)\}$ erzeugt alle Permutationen auf $\underline{n}$, denn:

- wegen $(12\ldots n)^{n-1}(12\ldots n) = (1)(2)\ldots(n)$ gilt $(12\ldots n)^{-1} = (12\ldots n)^{n-1}$,
- Transpositionen der Form $(k-1k)$ erhält man durch $(k-1k) = (12\ldots n)^{-(k-2)}(12)(12\ldots n)^{(k-2)}$,
- Transpositionen der Form $(1k)$ erhält man rekursiv, beginnend mit $k = 3$, durch $(1k) = (1k-1)(k-1k)(1k-1)$,
- Transpositionen der Form (xy) erhält man durch $(xy) = (1x)(1y)(1x)$,
- jeder Zyklus $(x_1x_2x_3\ldots x_k)$ läßt sich als Produkt von Transpositionen schreiben: $(x_1x_2x_3\ldots x_k) = (x_1x_2)(x_1x_3)\ldots(x_1x_k)$,
- jede Permutation läßt sich als Produkt elementfremder Zyklen schreiben.

Gäbe es ein Erzeugendensystem für $\mathbf{S}_n$ mit nur einem Element, so wäre $\mathbf{S}_n$ eine zyklische (Halb-)Gruppe, was nicht der Fall ist. □

3.9 Lemma *Jedes minimale Erzeugendensystem für $\mathbf{S}_n$ ist in $\mathbf{S}_n$ enthalten.*

Beweis: Sei A ein minimales Erzeugendensystem für $\mathbf{S}_n$. Angenommen $A \not\subseteq \mathbf{S}_n$, dann existiert ein $\alpha \in A \setminus \mathbf{S}_n$. Weil $\mathbf{S}_n \subseteq \langle A \rangle$ gilt, existieren für jedes $\mu \in \mathbf{S}_n$ Elemente $\alpha_1, \ldots, \alpha_k \in A$ mit $\mu = \alpha_1 \cdot \ldots \cdot \alpha_k$. Gäbe es ein $i \in \underline{k}$ mit $\alpha_i = \alpha \notin \mathbf{S}_n$, so wäre das Produkt nach Lemma 1.32 auf Seite 13 keine Permutation. Da dies $\mu \in \mathbf{S}_n$ widerspricht, sind alle α_i ungleich α und damit auch in der Menge $A \setminus \{\alpha\}$ enthalten. Daraus folgt, daß $\mu \in \langle A \setminus \{\alpha\} \rangle$ und damit $\mathbf{S}_n \subseteq \langle A \setminus \{\alpha\} \rangle$ gilt, wobei $A \setminus \{\alpha\}$ eine echte Teilmenge von A ist. Damit ist A kein minimales Erzeugendensystem für $\mathbf{S}_n$ und folglich ist die Annahme falsch, d.h. es gilt $A \subseteq \mathbf{S}_n$ und das Lemma ist bewiesen. □

3.10 Folgerung Wenn A ein Erzeugendensystem für $\mathbf{S}_n$ ist, dann gilt: $\langle A \cap \mathbf{S}_n \rangle = \mathbf{S}_n$. Denn weil $\mathbf{S}_n$ ein Untermonoid von $\mathbf{B}_n$ und demnach abgeschlossen bezüglich der Matrizenmultiplikation ist, gilt $\langle A \cap \mathbf{S}_n \rangle \subseteq \mathbf{S}_n$. Betrachtet man eine minimale Teilmenge von A, welche $\mathbf{S}_n$ erzeugt, so ist diese nach dem vorhergehenden Lemma in $\mathbf{S}_n$ und auch in $A \cap \mathbf{S}_n$ enthalten. Daher gilt $\mathbf{S}_n \subseteq \langle A \cap \mathbf{S}_n \rangle$.

B. Das von den regulären Matrizen erzeugte Untermonoid

Als Hauptresultat dieses Abschnittes folgt nun der Satz von Kim und Roush [KR77] über ein minimales Erzeugendensystem für das von den regulären Elementen von $\mathbf{B}_n$ erzeugte Untermonoid $\mathbf{B}_n^r$.

3.11 Definition Sei $R \subseteq \mathbf{B}_n$ die Menge aller regulären Elemente von $\mathbf{B}_n$, d.h.

$$R := \{\alpha \in \mathbf{B}_n \mid \exists \beta \in \mathbf{B}_n : \alpha = \alpha\beta\alpha\}.$$

Dann bezeichnen wir mit $\mathbf{B}_n^r$ das von R erzeugte Untermonoid, d.h. $\mathbf{B}_n^r := \langle R \rangle$.

3.12 Satz ([KR77]) *Seien τ und π die in 2.3 auf Seite 15 definierten Matrizen vom Typ t bzw. p und $\mathfrak{M}$ ein minimales Erzeugendensystem für $\mathbf{S}_n$. Dann ist die Menge $\mathfrak{A} := \{\tau, \pi\} \cup \mathfrak{M}$ ein minimales Erzeugendensystem für $\mathbf{B}_n^r$.*

Beweis: Wir zeigen in mehreren Schritten, wie man jede reguläre Boolesche Matrix aus einer Permutation erzeugen kann, indem man die Permutationsmatrix sukzessive mit geeigneten Matrizen multipliziert. Dazu gehen wir rückwärts vor, d.h. die Permutation erhalten wir erst am Ende des Beweises.
Bevor wir damit beginnen, stellen wir fest, daß wir neben $\mathbf{S}_n$ auch alle Matrizen vom Typ t und vom Typ p erzeugen können (siehe Lemma 2.5 auf Seite 16). Daher können wir beliebige Zeilen einer Matrix „aufaddieren“ bzw. „löschen“ (siehe Bemerkungen 2.9 auf Seite 17 und 2.11 auf Seite 18), indem wir die Ausgangsmatrix mit geeigneten Matrizen vom Typ t bzw. p multiplizieren.
Sei nun eine reguläre Matrix $\alpha \in \mathbf{B}_n$ gegeben.

Schritt 1: Wir ersetzen alle Zeilen von α, die $\bigvee$-reduzibel in $\mathfrak{Z}(\alpha)$ sind (also Supremum anderer Zeilen von α sind), durch den Nullvektor und erhalten somit die Matrix β (gleiche Zeilen, die $\bigvee$-irreduzibel sind, ersetzen wir alle bis auf jeweils eine durch den Nullvektor). Aus β läßt sich durch Aufaddieren geeigneter Zeilen die Matrix α erzeugen. Dies ist nach Bemerkung 2.9 auf Seite 17 durch fortgesetzte Multiplikation mit entsprechenden Matrizen vom Typ t möglich.

Durch das Löschen $\bigvee$-reduzibler Zeilen einer Matrix ändert sich der Zeilenverband nicht, d.h. $\mathfrak{Z}(\alpha) = \mathfrak{Z}(\beta)$ und weil $\mathfrak{Z}(\alpha)$ wegen der Regularität von α nach Zareckis Kriterium 2.21 auf Seite 25 vollständig distributiv ist, ist dies auch $\mathfrak{Z}(\beta)$ und damit ist β regulär.

Schritt 2: Wir wenden Lemma 2.23 auf Seite 26 auf β an und erhalten somit eine Menge A_β von Zeilen von β und entsprechende Einheitsvektoren u_i für jede Zeile $\beta_{i*} \in A_\beta$ (die u_i haben nicht zwangsläufig an der i-ten Stelle eine Eins, der Index gibt vielmehr die zugehörige Zeile an). Da im vorherigen Schritt gleiche $\bigvee$-irreduzible Zeilen alle bis auf je eine durch Nullvektoren ersetzt wurden, gibt es keine zwei u_i, die gleich sind.

Jetzt ersetzen wir die Nullzeilen in β durch diejenigen Einheitsvektoren, welche sich nicht unter den u_i befinden und erhalten die Matrix γ. Dann gilt: $\beta = \tilde{\pi}\gamma$, wobei $\tilde{\pi}$ ein Produkt von solchen Matrizen des Typs p ist, wie sie in Bemerkung 2.11 auf Seite 18 genannt werden. Durch $\tilde{\pi}$ werden die geänderten Zeilen in γ durch Nullvektoren ersetzt.

Die Zeilen A_β zusammen mit den neuen Einheitsvektoren ergeben für γ eine Menge A_γ gemäß Lemma 2.23 auf Seite 26. Die Menge der u_i für A_γ enthält dann alle n Einheitsvektoren, denn wir haben ja gerade jene gewählt, die sich noch nicht unter den u_i für β befanden. Damit ist γ regulär und weil nach Konstruktion keine zwei Zeilen gleich und in γ alle Zeilen $\bigvee$-irreduzibel sind, hat γ maximalen Zeilenrang.

Folgende Interpretation für die u_i kann zum Verständnis des nächsten Schrittes beitragen: jeder Zeile γ_{i*} ist ja ein u_i zugeordnet und dieses enthält genau eine Eins an der Stelle j_i. Stellen wir uns nun die Einsen γ_{ij_i} „angemalt“ vor, dann sind es genau jene Einsen, die am Ende von Schritt 3 in der Matrix übrig bleiben und die Ausgangspermutation bilden.

Schritt 3: Wenn es in γ noch Zeilenpaare γ_{a*} und γ_{b*} mit $\gamma_{b*} > \gamma_{a*}$ gibt, dann sei γ_{c*} eine minimale Zeile, die größer als γ_{a*} ist, das heißt aus $\gamma_{c*} \geq \gamma_{i*} > \gamma_{a*}$ folgt $i = c$ (für alle $i \in \underline{n}$). Da keine zwei Zeilen von γ gleich sind, kann ein solches c gewählt werden.

Wir erhalten die Matrix $\hat{\gamma}$, indem wir in γ die Zeile γ_{c*} durch den Vektor $\gamma_{c*} \ominus u_a$ ersetzen, wobei $(\gamma_{c*} \ominus u_a)_j = 1$ genau dann, wenn $(u_a)_j = 0$ und $(\gamma_{c*})_j = 1$ (siehe Definition 1.19 auf Seite 7). Dann gilt: $\hat{\gamma}_{c*} < \gamma_{c*}$.

Umgekehrt erhalten wir γ aus $\hat{\gamma}$, indem wir durch Multiplikation mit einer Matrix vom Typ t die c-te Zeile von $\hat{\gamma}$ durch das Supremum der a-ten mit der c-ten Zeile von $\hat{\gamma}$ ersetzen: $\gamma = T^{ca}\hat{\gamma}$ (siehe Bemerkung 2.9 auf Seite 17).

Nun ist $\hat{\gamma}$ noch auf Regularität zu prüfen. Dazu zeigen wir, daß $\hat{\gamma}$ die Kriterien von Lemma 2.23 auf Seite 26 erfüllt. Die Menge der u_i bleibt die gleiche wie für γ und die Bedingungen (1) und (2) sind in jedem Fall erfüllt.

Da sich γ und $\hat{\gamma}$ nur in der c-ten Zeile voneinander unterscheiden, kann Bedingung (3) nur im Fall $i = c$ oder $j = c$ verletzt sein. Angenommen, $i = c$ und es existiert ein j mit $u_c \leq \hat{\gamma}_{j*} = \gamma_{j*}$. Dann gilt wegen der Regularität von γ die Ungleichung $\gamma_{c*} \leq \gamma_{j*}$ und wegen $\hat{\gamma}_{c*} \leq \gamma_{c*}$ dann auch: $\hat{\gamma}_{c*} \leq \hat{\gamma}_{j*}$.

Betrachten wir den Fall $j = c$ und nehmen an, es gibt ein u_i mit $u_i \leq \hat{\gamma}_{c*} < \gamma_{c*}$ aber $\hat{\gamma}_{i*} \not\leq \hat{\gamma}_{c*}$. Weil γ regulär ist, erfüllt es (3) und daher gilt: $\gamma_{i*} \leq \gamma_{c*}$. Des weiteren unterscheidet sich γ_{c*} von $\hat{\gamma}_{c*}$ nur durch u_a und folglich muß $u_a \leq \gamma_{i*}$ gelten. Mit der Regularität von γ folgern wir $\gamma_{a*} \leq \gamma_{i*}$ und weiter $\gamma_{a*} \leq \gamma_{i*} \leq \gamma_{c*}$. Wegen der Minimalität von γ_{c*} muß $i = a$ oder $i = c$ gelten. Im Fall $i = a$ gilt $u_a \leq \hat{\gamma}_{c*}$ nie und damit ist (3) erfüllt. Im Fall $i = c$ gilt $u_c \leq \hat{\gamma}_{c*}$ und $\hat{\gamma}_{c*} \leq \hat{\gamma}_{c*}$ stets und damit ist (3) ebenfalls erfüllt.

Die Matrix $\hat{\gamma}$ ist also regulär. Setzen wir $\gamma := \hat{\gamma}$, dann können wir mittels des 3. Schrittes die Anzahl an Einsen in γ solange reduzieren, bis es in γ keine Zeile mehr gibt, die größer als eine andere Zeile ist. Schließlich folgt dann aus $u_a \leq \gamma_{b*}$ stets $a = b$ und damit auch $u_a = \gamma_{a*}$.

Da die u_i gerade alle n Einheitsvektoren sind, ist γ eine Permutationsmatrix und es ist gezeigt, daß sich jede reguläre Matrix aus einer Permutationsmatrix durch Multiplikation mit Matrizen vom Typ t oder p erzeugen läßt.
Nun ist noch die Minimalität von $\mathfrak{A}$ zu zeigen. Sei also $\hat{\mathfrak{A}} \subseteq \mathfrak{A}$ ein Erzeugendensystem für $\mathbf{B}_n^r$. Wir zeigen, daß $\hat{\mathfrak{A}} = \mathfrak{A}$ gilt.
Da Permutationen regulär sind, folgt aus $\langle \hat{\mathfrak{A}} \rangle = \mathbf{B}_n^r$ und Folgerung 3.6 auf Seite 33: $\langle \hat{\mathfrak{A}} \cap \mathbf{S}_n \rangle = \mathbf{S}_n$. Nach Lemma 3.4 auf Seite 32 sind π und τ keine Permutationen und daher gilt: $\mathfrak{A} \cap \mathbf{S}_n \subseteq \mathfrak{M}$ und wegen Lemma 3.9 auf Seite 35 sogar $\mathfrak{A} \cap \mathbf{S}_n = \mathfrak{M}$. Mit $\hat{\mathfrak{A}} \cap \mathbf{S}_n \subseteq \mathfrak{A} \cap \mathbf{S}_n = \mathfrak{M}$ und $\langle \hat{\mathfrak{A}} \cap \mathbf{S}_n \rangle = \mathbf{S}_n$ und der Minimalität von $\mathfrak{M}$ folgt schließlich $\hat{\mathfrak{A}} \cap \mathbf{S}_n = \mathfrak{M}$ und damit ist $\mathfrak{M}$ in $\hat{\mathfrak{A}}$ enthalten.
Weil Matrizen vom Typ t nach Folgerung 2.20 auf Seite 25 regulär sind, muß $\hat{\mathfrak{A}}$ nach Lemma 2.17 auf Seite 22 und 3.5 auf Seite 33 eine Matrix δ vom Typ t enthalten. Nach Lemma 3.4 auf Seite 32 enthält $\mathbf{S}_n \cup \{\pi\}$ keine Matrizen vom Typ t und daher gilt $\mathfrak{A} \cap \mathcal{T} = \{\tau\}$. Aus $\delta \in (\hat{\mathfrak{A}} \cap \mathcal{T}) \subseteq (\mathfrak{A} \cap \mathcal{T}) = \{\tau\}$ folgt schließlich $\tau \in \hat{\mathfrak{A}}$.
Jetzt muß $\hat{\mathfrak{A}}$ noch eine Matrix mit einer Nullzeile enthalten, denn das Produkt von Matrizen ohne Nullzeilen ergibt stets wieder eine Matrix ohne Nullzeile. Da $\hat{\mathfrak{A}} \subseteq \mathfrak{A}$ gilt und π als einzige Matrix in $\mathfrak{A}$ eine Nullzeile hat, ist π in $\hat{\mathfrak{A}}$ enthalten und damit $\mathfrak{A}$ minimal, denn es folgt $\hat{\mathfrak{A}} = \mathfrak{A}$.
Schlußendlich erzeugt $\mathfrak{A}$ nicht nur ganz $\mathbf{B}_n^r$, sondern jedes Element daraus wird auch wirklich benötigt, um $\mathbf{B}_n^r$ zu erzeugen. Mit der Einschränkung natürlich, daß für τ und π jeweils andere Matrizen vom gleichen Typ genommen werden können. □

3.13 Beispiel Sei α die in Beispiel 2.22 auf Seite 25 definierte Matrix. Wir faktorisieren α nach und nach, wie im Beweis zu Satz 3.12:

Schritt 1

$$\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & \underline{1} & 0 \\ 0 & 1 & 1 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \underline{1} & 0 & 1 & 0 & 0 \end{pmatrix} = T^{41}T^{43}\beta$$

Also ist α als Produkt zweier Typ t Matrizen mit β darstellbar. Die unterstrichenen Einsen entsprechen der Eins im u_i für die jeweilige Zeile.

Schritt 2

$$\beta = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & \underline{1} & 0 \\ 0 & 1 & 1 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 1 & 0 & 0 \end{pmatrix} = P^4\gamma$$

Damit ist β als Produkt der Typ p Matrix P^4 (siehe Bemerkung 2.11 auf Seite 18) mit γ darstellbar und γ ist regulär mit maximalem Zeilenrang.

Schritt 3 Jetzt werden schrittweise „überflüssige“ Einsen in den Zeilen durch Nullen ersetzt. Diejenige Eins, welche ersetzt wird, ist durchgestrichen gezeichnet.

$$\gamma = \begin{pmatrix} 1 & 0 & 1 & \underline{1} & 0 \\ 0 & \not{1} & 1 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & \underline{1} & 0 \\ 0 & 0 & 1 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 1 & 0 & 0 \end{pmatrix} = T^{23}\gamma^{(1)}$$

$$\gamma^{(1)} = \begin{pmatrix} \not{1} & 0 & 1 & \underline{1} & 0 \\ 0 & 0 & 1 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & \underline{1} & 0 \\ 0 & 0 & 1 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 1 & 0 & 0 \end{pmatrix} = T^{15}\gamma^{(2)}$$

$$\gamma^{(2)} = \begin{pmatrix} 0 & 0 & 1 & \underline{1} & 0 \\ 0 & 0 & 1 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & \not{1} & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & \underline{1} & 0 \\ 0 & 0 & 1 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 0 & 0 & 0 \end{pmatrix} = T^{54}\gamma^{(3)}$$

$$\gamma^{(3)} = \begin{pmatrix} 0 & 0 & 1 & \underline{1} & 0 \\ 0 & 0 & \not{1} & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & \underline{1} & 0 \\ 0 & 0 & 0 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 0 & 0 & 0 \end{pmatrix} = T^{24}\gamma^{(4)}$$

$$\gamma^{(4)} = \begin{pmatrix} 0 & 0 & \not{1} & \underline{1} & 0 \\ 0 & 0 & 0 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & \underline{1} & 0 \\ 0 & 0 & 0 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & 0 & 0 \\ 0 & 0 & \underline{1} & 0 & 0 \\ \underline{1} & 0 & 0 & 0 & 0 \end{pmatrix} = T^{14}\gamma^{(5)}$$

Wir erhalten mit $\gamma^{(5)}$ eine Permutationsmatrix und folglich ergibt sich γ als Produkt: $\gamma = T^{23}T^{15}T^{54}T^{24}T^{14}\gamma^{(5)}$.

Damit läßt sich α schließlich schreiben als $\alpha = T^{41}T^{43}P^4T^{23}T^{15}T^{54}T^{24}T^{14}\gamma^{(5)}$.

C. Magere Matrizen mit maximalem Zeilen- und Spaltenrang

Folgendes Lemma ist die Grundlage für den Beweis des Satzes von Devadze und stammt von Konieczny:

3.14 Lemma ([Kon05]) *Für jede Matrix $\alpha \in \mathbf{B}_n$ existiert ein $\alpha^* \in \mathbf{B}_n$, so daß folgendes gilt:*

(1) *α^* ist mager,*

(2) *falls α^* eine Nullzeile hat, dann enthält jede Zeile von α^* maximal eine Eins,*

(3) *falls α^* eine Nullspalte hat, dann enthält jede Spalte von α^* maximal eine Eins,*

(4) $|\mathfrak{Z}(\alpha)| \leq |\mathfrak{Z}(\alpha^*)|$,

(5) $\alpha \in \langle \{\pi, \tau, \alpha^*\} \cup \mathbf{S}_n \rangle$,

Beweis:
Der Beweis beginnt mit einem Algorithmus zur Konstruktion einer Matrix α_{t+1} aus einer Matrix α_t. Dabei starten wir mit der Matrix α und konstruieren daraus sukzessive eine Matrix α^*, welche die Bedingungen des Lemmas erfüllt, also insbesondere mager ist.

(A) Sei $\alpha_0 := \alpha$ und $t := 0$ gesetzt.

(B) An dieser Stelle wurde α_t bereits konstruiert und α_{t+1} sei folgendermaßen definiert:

a) *Falls es in α_t eine Zeile gibt, die nicht minimal ist, dann entfernen wir in einer Zeile, die größer ist als diese, alle Einsen, die in der kleineren Zeile enthalten sind.*

Falls i und j existieren mit $i \neq j$ und $(\alpha_t)_{j*} \neq \mathbf{0}$ und $(\alpha_t)_{j*} \leq (\alpha_t)_{i*}$ dann setzen wir

$$(\alpha_{t+1})_{k*} := \begin{cases} (\alpha_t)_{i*} \ominus (\alpha_t)_{j*} & \text{falls } k = i \\ (\alpha_t)_{k*} & \text{sonst} \end{cases}$$

und $t := t + 1$ und gehen zurück zu Schritt (B).

b) *Falls es in α_t eine Nullzeile gibt und eine weitere Zeile, die mehr als eine Eins enthält, dann entfernen wir eine der Einsen und setzen sie an gleicher Stelle in die Nullzeile.*

Falls i und j existieren mit $|(\alpha_t)_{i*}| \geq 2$ und $(\alpha_t)_{j*} = \mathbf{0}$, dann wählen wir ein l mit $(\alpha_t)_{il} = 1$ und setzen

$$(\alpha_{t+1})_{k*} := \begin{cases} (\alpha_t)_{i*} \ominus e^{(l)} & \text{falls } k = i \\ e^{(l)} & \text{falls } k = j \\ (\alpha_t)_{k*} & \text{sonst} \end{cases}$$

und $t := t + 1$ und gehen zurück zu Schritt (B).

c) Wir führen Schritt (a) analog mit den Spalten aus.

d) Wir führen Schritt (b) analog mit den Spalten aus.

e) Wir setzen $\alpha_{t+1} := \alpha_t$ und beenden die Konstruktion.

Zunächst ist zu zeigen, daß der Schritt e) überhaupt ausgeführt wird, die Konstruktion also terminiert. In den Schritten a) und c) nimmt die Anzahl der Einsen in der Matrix stets ab, d.h. $|\alpha_{t+1}| < |\alpha_t|$. In den Schritten b) und d) bleibt die Anzahl der Einsen gleich, d.h. $|\alpha_{t+1}| = |\alpha_t|$, die Anzahl an Nullzeilen bzw. -spalten wird jedoch kleiner:

$$|\{i : (\alpha_{t+1})_{i*} = \mathbf{0}\}| + |\{j : (\alpha_{t+1})_{*j} = \mathbf{0}\}| \quad < \quad |\{i : (\alpha_t)_{i*} = \mathbf{0}\}| + |\{j : (\alpha_t)_{*j} = \mathbf{0}\}|.$$

Da α_t nur endlich viele Einsen und Nullzeilen bzw. Nullspalten haben kann, existiert ein m so daß $\alpha_m = \alpha_{m+1}$ gilt.
Sei $\alpha^* := \alpha_m$. Wir zeigen, daß α^* die geforderten Eigenschaften hat.
Die Matrix α^* ist mager, weil alle Zeilen und Spalten von α^* minimal sind. Denn gäbe es eine Zeile $(\alpha_m)_{i*}$ und eine andere Zeile $(\alpha_m)_{j*} \neq \mathbf{0}$ mit $(\alpha_m)_{j*} \leq (\alpha_m)_{i*}$, dann hätte Schritt a) ausgeführt werden können und es wäre $\alpha_m \neq \alpha_{m+1}$. Ebenso zeigt man, daß alle Spalten von α^* minimal sind – (1) gilt also.
Angenommen, α^* enthält eine Nullzeile. Gäbe es dann eine weitere Zeile, die mehr als eine Eins enthält, dann hätte Schritt b) ausgeführt werden können und α_m wäre ungleich α_{m+1}. Falls α^* also eine Nullzeile enthält, dann hat jede andere Zeile von α^* maximal eine Eins. Damit ist (2) gezeigt und mit einer analogen Argumentation zeigt man (3).
Sei $t \geq 0$ und α_{t+1} definiert durch die Schritte a) oder b). Dann läßt sich jede Zeile von α_t als Supremum von Zeilen von α_{t+1} darstellen und daher gilt: $\mathfrak{Z}(\alpha_t) \subseteq \mathfrak{Z}(\alpha_{t+1})$. Ist α_{t+1} durch die Schritte c) oder d) definiert, so läßt sich jede Spalte von α_t als Supremum von Spalten von α_{t+1} darstellen und deshalb gilt $\mathfrak{S}(\alpha_t) \subseteq \mathfrak{S}(\alpha_{t+1})$ und nach Punkt (1) von Lemma 1.31 auf Seite 10 auch $|\mathfrak{Z}(\alpha_t)| \leq |\mathfrak{Z}(\alpha_{t+1})|$. Ist α_{t+1} durch den Schritt e) definiert, so gilt $\mathfrak{Z}(\alpha_t) = \mathfrak{Z}(\alpha_{t+1})$. Damit gilt nach jedem Schritt $|\mathfrak{Z}(\alpha_t)| \leq |\mathfrak{Z}(\alpha_{t+1})|$ und per Induktion über t ergibt sich $|\mathfrak{Z}(\alpha)| \leq |\mathfrak{Z}(\alpha^*)|$, Punkt (4) gilt demnach ebenfalls.
Nun bleibt noch Punkt (5) zu zeigen. Dazu betrachten wir, wie man in jedem der Schritte a) bis d) „rückwärts“ geht, das heißt wie man aus der Matrix α_{t+1} die Matrix α_t erhält:

(a) $\alpha_t = T^{ij}\alpha_{t+1}$ *(Aufaddieren der j-ten Zeile auf die i-te Zeile)*

(b) $\alpha_t = P^j(T^{ij}\alpha_{t+1})$ *(Aufaddieren der j-ten Zeile auf die i-te Zeile und anschließendes Löschen der j-ten Zeile)*

(c) $\alpha_t = \alpha_{t+1}T^{ji}$ *(Aufaddieren der j-ten Spalte auf die i-te Spalte)*

(d) $\alpha_t = (\alpha_{t+1}T^{ji})P^j$. *(Aufaddieren der j-ten Spalte auf die i-te Spalte und anschließendes Löschen der j-ten Spalte)*

Dabei sind T^{ij}, T^{ji} und P^j jene Matrizen vom Typ t bzw. p, wie sie in 2.8 auf Seite 17 und 2.10 auf Seite 18 definiert wurden. In jedem Schritt gilt also $\alpha_t \in \langle\{\pi, \tau, \alpha_{t+1}\} \cup \mathbf{S}_n\rangle$, denn darin sind neben α_{t+1} auch alle Matrizen vom Typ t und p enthalten. Per Induktion ergibt sich, daß α stets in $\langle\{\pi, \tau, \alpha^*\} \cup \mathbf{S}_n\rangle$ enthalten ist und damit (5) gilt. □
Das folgende Lemma stellt den letzten wichtigen Baustein zum Beweis des Theorems von Devadze dar und wurde ebenfalls von Prof. Konieczny bewiesen. Es gibt ein Erzeugendensystem für die Menge aller mageren Matrizen mit maximalem Zeilen- und Spaltenrang an.

3.15 Lemma ([Kon05]) *Sei $\mathfrak{P}$ eine Menge, die aus jeder primen $\mathscr{D}$-Klasse eine Matrix enthält. Dann enthält das Untermonoid $U := \langle\{\tau, \pi\} \cup \mathbf{S}_n \cup \mathfrak{P}\rangle$ von $\mathbf{B}_n$ alle mageren Matrizen mit maximalem Zeilen- und Spaltenrang.*

Beweis: Sei M die Menge aller mageren Matrizen mit maximalem Zeilen- und Spaltenrang. Zum Beweis des Lemmas nehmen wir an, daß M nicht in U enthalten ist und führen dies zum Widerspruch. Sei zunächst m folgendermaßen definiert:

$$m := \max_{\alpha \in M \setminus U} |\mathfrak{Z}(\alpha)|$$

und $\alpha \in M \setminus U$ eine Matrix, für die $|\mathfrak{Z}(\alpha)| = m$ gilt. Das Maximum m existiert, denn $M \setminus U$ ist laut Annahme nicht leer und jeder Zeilenverband kann maximal 2^n Elemente haben.
Die Matrix α ist nicht in U enthalten und damit ist α nicht prim und auch keine Permutationsmatrix. Denn U enthält ja ganz $\mathbf{S}_n$ und aus jeder primen $\mathscr{D}$-Klasse eine Matrix und deshalb alle primen Matrizen. Daher existieren $\beta, \gamma \in \mathbf{B}_n \setminus \mathbf{S}_n$ mit $\alpha = \beta\gamma$ und nach (2) und (3) von Lemma 1.31 auf Seite 10 gilt dann $\mathfrak{Z}(\alpha) \subseteq \mathfrak{Z}(\gamma)$ und $\mathfrak{S}(\alpha) \subseteq \mathfrak{S}(\beta)$.
Es gilt sogar $\mathfrak{Z}(\alpha) \subsetneq \mathfrak{Z}(\gamma)$, denn angenommen, $\mathfrak{Z}(\alpha) = \mathfrak{Z}(\gamma)$. Dann folgt aus (4) von Lemma 1.31 auf Seite 10: $\mathfrak{Z}_B(\alpha) = \mathfrak{Z}_B(\gamma)$ und weil α maximalen Zeilenrang hat, enthält die Zeilenbasis n Elemente, also alle Zeilen von α. Damit enthält aber auch $\mathfrak{Z}_B(\gamma)$ alle Zeilen von α und somit ist γ lediglich eine Umordnung der Zeilen von α, also β eine Permutation. Dies steht im Widerspruch zu $\beta \in \mathbf{B}_n \setminus \mathbf{S}_n$ und daher gilt $\mathfrak{Z}(\alpha) \neq \mathfrak{Z}(\gamma)$ und damit $|\mathfrak{Z}(\alpha)| < |\mathfrak{Z}(\gamma)|$. Analog kann man zeigen, daß $\mathfrak{S}(\alpha) \subsetneq \mathfrak{S}(\beta)$ gilt, woraus nach Punkt (1) von Lemma 1.31 auf Seite 10 die Ungleichung $|\mathfrak{Z}(\alpha)| < |\mathfrak{Z}(\beta)|$ folgt.
Sei γ^* eine Matrix, die die Bedingungen in Lemma 3.14 auf Seite 39 für γ erfüllt.
Angenommen, γ^* hat eine Nullzeile. Dann hat es wegen 3.14(2) maximal eine Eins pro Zeile und daher auch eine Nullspalte und somit wegen 3.14(3) maximal eine Eins pro Spalte. Nach Bemerkung 2.12 auf Seite 18 läßt sich γ^* dann als Produkt von Matrizen des Typs p darstellen und daher gilt $\gamma^* \in \langle\{\pi\} \cup \mathbf{S}_n\rangle$.

Angenommen, γ^* hat keine Nullzeile (und damit auch keine Nullspalte), dann hat γ^*, weil es mager ist, nach Bemerkung 1.30 auf Seite 10 maximalen Zeilen- und Spaltenrang. Folglich ist γ^* in U enthalten, denn es gilt: $m = |\mathfrak{Z}(\alpha)| < |\mathfrak{Z}(\gamma)| \leq |\mathfrak{Z}(\gamma^*)|$.
Zusammengefasst gilt dann mit Punkt (5) von Lemma 3.14:

$$\gamma \in \langle \{\pi, \tau, \gamma^*\} \cup \mathbf{S}_n \rangle \subseteq \langle \{\pi, \tau, \gamma^*\} \cup \mathbf{S}_n \cup \mathfrak{P} \rangle \subseteq U.$$

Auf ähnliche Weise zeigt man für eine Matrix β^*, welche die Bedingungen in Lemma 3.14 auf Seite 39 erfüllt, daß $\beta^* \in U$ und damit auch $\beta \in U$ gilt. Wegen $\gamma \in U$ gilt dann aber $\alpha = \beta\gamma \in U$ im Widerspruch zur Annahme, daß M nicht in U enthalten ist. Folglich muß M alle Matrizen mit maximalem Zeilen- und Spaltenrang enthalten. □

4. Das Theorem von Devadze

Als Hauptresultat der vorliegenden Arbeit folgt nun das Theorem von Devadze über Erzeugendensysteme Boolescher Matrizen. Dieses wurde von H. M. Devadze im Jahre 1968 in [Dev68] ohne Beweis veröffentlicht. Prof. Konieczny vom Mary Washington College (Fredericksburg, USA) bewies die Aussage (1) des Theorems in seiner Dissertation [Kon92], eine „self-contained"-Version wird bald erscheinen [Kon05].

4.1 Theorem *Sei*

- $\mathfrak{M}$ *ein minimales Erzeugendensystem für* $\mathbf{S}_n$,
- π *eine beliebige Matrix vom Typ* p,
- τ *eine beliebige Matrix vom Typ* t,
- ϱ *eine beliebige Matrix vom Typ* r,
- ϱ' *eine beliebige Matrix vom Typ* r',
- $\mathfrak{P}$ *eine Menge, die aus jeder primen* $\mathscr{D}$*-Klasse genau eine Matrix enthält.*

Dann gilt:

(1) die Menge $\mathfrak{A}_1 := \mathfrak{M} \cup \mathfrak{P} \cup \{\pi, \tau\}$ *ist ein minimales Erzeugendensystem für* $\mathbf{B}_n$,

(2) die Menge $\mathfrak{A}_2 := \mathfrak{M} \cup \mathfrak{P} \cup \{\varrho, \varrho', \tau\}$ *ist ein minimales Erzeugendensystem für* $\mathbf{B}_n$,

(3) in jedem Erzeugendensystem für $\mathbf{B}_n$ *ist eine Menge der Form (1) oder (2) enthalten.*

Beweis: Zunächst einige Vorbemerkungen:

(a) Da $\mathfrak{M}$ ein minimales Erzeugendensystem für $\mathbf{S}_n$ ist, gilt nach Lemma 3.9 auf Seite 35: $\mathfrak{M} \subseteq \mathbf{S}_n$.
(b) Nach Folgerung 3.6 auf Seite 33 sind alle Matrizen in $\mathfrak{P}$ prim.

(c) Damit gilt nach Lemma 3.4 auf Seite 32:

$$\begin{aligned}\mathfrak{A}_1 \cap \{\alpha \in \mathbf{B}_n \mid \alpha \text{ ist prim }\} = \mathfrak{A}_2 \cap \{\alpha \in \mathbf{B}_n \mid \alpha \text{ ist prim }\} &= \mathfrak{P},\\ \mathfrak{A}_1 \cap \mathbf{S}_n = \mathfrak{A}_2 \cap \mathbf{S}_n &= \mathfrak{M},\\ \mathfrak{A}_1 \cap \mathcal{T} = \mathfrak{A}_2 \cap \mathcal{T} &= \{\tau\},\\ \mathfrak{A}_1 \cap \mathcal{P} &= \{\pi\},\\ \mathfrak{A}_2 \cap \mathcal{R} &= \{\varrho\},\\ \mathfrak{A}_2 \cap \mathcal{R}' &= \{\varrho'\},\\ \mathfrak{A}_1 \cap \mathcal{R} = \mathfrak{A}_1 \cap \mathcal{R}' = \mathfrak{A}_2 \cap \mathcal{P} &= \emptyset.\end{aligned}$$

Zunächst zeigen wir, daß $\mathfrak{A}_1$ ein Erzeugendensystem für $\mathbf{B}_n$ ist und beweisen danach dessen Minimalität. Schließlich zeigen wir die Aussagen (2) und (3) des Theorems.

(1) Zuerst ist zu bemerken, daß $\langle\mathfrak{A}_1\rangle$ nach Lemma 2.5 auf Seite 16 alle Matrizen der Typen p und t enthält und wir daher auch annehmen können, daß π und τ die in 2.3 auf Seite 15 definierten Matrizen sind.

Sei $\alpha \in \mathbf{B}_n$ und α^* genüge den Bedingungen in Lemma 3.14 auf Seite 39. Dann ist α^* entweder mager mit maximalem Zeilen- und Spaltenrang oder jede Zeile und jede Spalte von α^* enthält maximal eine Eins.

Im ersten Fall ist α^* nach Lemma 3.15 auf Seite 41 in $\langle\mathfrak{A}_1\rangle$ enthalten und im zweiten Fall gilt nach Bemerkung 2.12 auf Seite 18: $\alpha^* \in \langle\{\pi\} \cup \mathbf{S}_n\rangle \subseteq \langle\mathfrak{A}_1\rangle$. Demnach gilt $\alpha^* \in \langle\mathfrak{A}_1\rangle$ und nach Punkt (5) von Lemma 3.14 auf Seite 39 folgt: $\alpha \in \langle\{\pi, \tau, \alpha^*\} \cup \mathbf{S}_n\rangle \subseteq \langle\mathfrak{A}_1\rangle$. Also ist $\mathfrak{A}_1$ ein Erzeugendensystem für $\mathbf{B}_n$.

Um zu zeigen, daß $\mathfrak{A}_1$ minimal ist, nehmen wir an, daß es eine Menge $\hat{\mathfrak{A}}$ mit $\langle\hat{\mathfrak{A}}\rangle = \mathbf{B}_n$ und $\hat{\mathfrak{A}} \subseteq \mathfrak{A}_1$ gibt und zeigen, daß dann $\hat{\mathfrak{A}} = \mathfrak{A}_1$ gilt.

Zunächst zeigen wir, daß $\mathfrak{M}$ in $\hat{\mathfrak{A}}$ enthalten sein muß. Wegen $\langle\hat{\mathfrak{A}}\rangle = \mathbf{B}_n$ gilt nach Folgerung 3.10 auf Seite 35: $\langle\hat{\mathfrak{A}} \cap \mathbf{S}_n\rangle = \mathbf{S}_n$. Mit Vorbemerkung (c) ergibt sich $\hat{\mathfrak{A}} \cap \mathbf{S}_n \subseteq \mathfrak{A}_1 \cap \mathbf{S}_n = \mathfrak{M}$ und wegen der Minimalität von $\mathfrak{M}$ schließlich $\hat{\mathfrak{A}} \cap \mathbf{S}_n = \mathfrak{M}$. Damit ist $\mathfrak{M}$ in $\hat{\mathfrak{A}}$ enthalten.

Sei $\alpha \in \mathfrak{P}$ und D_α die zugehörige prime $\mathscr{D}$-Klasse. Dann besagt Folgerung 3.6 auf Seite 33, daß $\hat{\mathfrak{A}}$ eine Matrix $\beta \in D_\alpha$ enthält. Da α als einziges Element aus D_α in $\mathfrak{P}$ enthalten ist, gilt $\mathfrak{P} \cap D_\alpha = \{\alpha\}$. Weil alle Elemente in D_α prim sind folgt mit Vorbemerkung (c): $\mathfrak{A}_1 \cap D_\alpha \subseteq \mathfrak{P}$. Es folgt $\{\alpha\} \subseteq \mathfrak{A}_1 \cap D_\alpha \subseteq \mathfrak{P} \cap D_\alpha = \{\alpha\}$ und daher $\mathfrak{A}_1 \cap D_\alpha = \{\alpha\}$. Zusammengefaßt ergibt sich: $\beta \in \hat{\mathfrak{A}} \cap D_\alpha \subseteq \mathfrak{A}_1 \cap D_\alpha = \{\alpha\}$, also $\beta = \alpha$ und somit ist jedes $\alpha \in \mathfrak{P}$ in $\hat{\mathfrak{A}}$ enthalten, also auch $\mathfrak{P}$.

Lemma 2.17 auf Seite 22 zusammen mit Lemma 3.5 auf Seite 33 besagt, daß $\hat{\mathfrak{A}}$ eine Matrix α vom Typ t enthalten muß. Mit Vorbemerkung (c) erhält man: $\alpha \in \hat{\mathfrak{A}} \cap \mathcal{T} \subseteq \mathfrak{A}_1 \cap \mathcal{T} = \{\tau\}$, also $\tau \in \hat{\mathfrak{A}}$.

Bisher haben wir gezeigt, daß $\{\tau\} \cup \mathfrak{P} \cup \mathfrak{M} \subseteq \hat{\mathfrak{A}}$ gilt. Nach der Vorbemerkung (c) enthält $\mathfrak{A}_1$ keine Matrix vom Typ r oder r′ und π ist als einzige Matrix vom Typ

p. Damit muß $\hat{\mathfrak{A}}$ nach Lemma 3.7 auf Seite 33 die Matrix π enthalten, denn sonst wäre es kein Erzeugendensystem für $\mathbf{B}_n$ oder keine Teilmenge von $\mathfrak{A}_1$.

Folglich gilt $\mathfrak{A}_1 \subseteq \hat{\mathfrak{A}}$ und daher ist $\mathfrak{A}_1$ ein minimales Erzeugendensystem.

(2) Nach Lemma 2.5 auf Seite 16 enthält $\langle\mathfrak{A}_2\rangle$ alle Matrizen der Typen r und r′ und daher können wir annehmen, daß ϱ und ϱ' die in 2.3 auf Seite 15 definierten Matrizen sind. Dann ist nach Bemerkung 2.7 auf Seite 17 das Produkt $\varrho\varrho' = \pi$ und damit alle Matrizen vom Typ p in $\langle\mathfrak{A}_2\rangle$ enthalten, weshalb $\mathfrak{A}_1 \subseteq \langle\mathfrak{A}_2\rangle$ gilt. Wie schon gezeigt wurde, erzeugt $\mathfrak{A}_1$ ganz $\mathbf{B}_n$ und weil $\langle\rangle$ ein isotoner und idempotenter Operator von $2^{\mathbf{B}_n}$ nach $2^{\mathbf{B}_n}$ ist, ist auch $\mathfrak{A}_2$ ein Erzeugendensystem für $\mathbf{B}_n$.

Sei $\hat{\mathfrak{A}}$ ein Erzeugendensystem für $\mathbf{B}_n$ und es gelte $\hat{\mathfrak{A}} \subseteq \mathfrak{A}_2$. Mit den gleichen Argumenten wie bei $\mathfrak{A}_1$ können wir folgern, daß $\{\tau\} \cup \mathfrak{P} \cup \mathfrak{M} \subseteq \hat{\mathfrak{A}}$ gilt.

Des weiteren enthält $\mathfrak{A}_2$ keine Matrix vom Typ p und ϱ ist als einzige Matrix vom Typ r und ϱ' als einzige vom Typ r′. Damit muß $\hat{\mathfrak{A}}$ nach Lemma 3.7 auf Seite 33 die Matrizen ϱ und ϱ' enthalten, denn sonst wäre es keine Teilmenge von $\mathfrak{A}_2$ oder kein Erzeugendensystem für $\mathbf{S}_n$.

Folglich gilt $\mathfrak{A}_2 \subseteq \hat{\mathfrak{A}}$ und daher ist $\mathfrak{A}_2$ ein minimales Erzeugendensystem.

(3) Aus dem bisher gezeigten folgt schon, daß jedes Erzeugendensystem für $\mathbf{B}_n$ eine Menge der Form $\mathfrak{A}_1$ oder $\mathfrak{A}_2$ enthält. Denn es muß aus jeder primen $\mathscr{D}$-Klasse eine Matrix enthalten und eine erzeugende Menge für $\mathbf{S}_n$, welche eine minimale erzeugende Menge für $\mathbf{S}_n$ enthält. Des weiteren eine Matrix vom Typ t und eine Matrix vom Typ p oder je eine Matrix vom Typ r und r′. Damit enthält es auch alle „Zutaten“, die $\mathfrak{A}_1$ oder $\mathfrak{A}_2$ enthält.

Schlußendlich ist hiermit das Theorem von Devadze bewiesen und für jede Menge ein Erzeugendensystem für das Monoid aller binären Relationen auf dieser Menge konstruierbar. □

Zu bemerken ist, daß jedes Erzeugendensystem für $\mathbf{B}_n$ aus einem Erzeugendensystem für das Monoid aller regulären Matrizen $\mathbf{B}_n^r$ und einem Repräsentanten jeder primen $\mathscr{D}$-Klasse besteht. Nach Bemerkung 2.35 auf Seite 30 wächst die Anzahl der primen $\mathscr{D}$-Klassen exponentiell und somit steigt mit wachsendem n auch die Größe der Erzeugendensysteme für $\mathbf{B}_n$ exponentiell an.

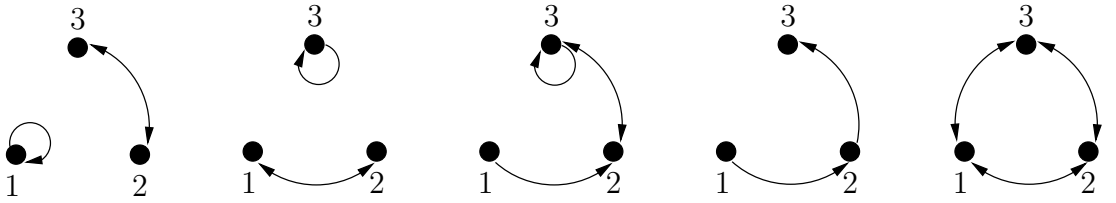
Beispielsweise enthält das von den regulären Elementen von $\mathbf{B}_4$ erzeugte Untermonoid $\mathbf{B}_4^r$ genau 63.904 Elemente, wovon 40.408 regulär sind [Kon02]. Alle darin enthaltenen Elemente lassen sich bereits durch vier der in Satz 3.12 auf Seite 35 genannten Matrizen erzeugen. Zur Erzeugung des gesamten Monoids $\mathbf{B}_n$ mit 65.536 Elementen sind zusätzlich Repräsentanten jeder der drei primen $\mathscr{D}$-Klassen hinzuzunehmen. Das Monoid $\mathbf{B}_5^r$ hat 32.311.832 Elemente, davon sind 8.683.982 regulär [Kon94] und wird ebenfalls von vier Matrizen erzeugt. Die Erzeugung aller $2^{25} = 33.554.432$ Elemente von $\mathbf{B}_5$ erfordert die Hinzunahme neun primer Matrizen zum Erzeugendensystem für $\mathbf{B}_5^r$.

4.2 Beispiel Abschließend ist ein Erzeugendensystem für $\mathbf{B}_3$ abgebildet. Dabei sind μ und ν Permutationen, die ganz $\mathbf{S}_3$ erzeugen. Die Matrix α ist prim und τ und π

sind Matrizen vom Typ t bzw. p. Unter den Matrizen sind die zugehörigen gerichteten Graphen zu sehen.

μ ν τ π α

$$\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix} \quad \begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix} \quad \begin{pmatrix}0&1&0\\0&0&1\\1&1&0\end{pmatrix} \quad \begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix} \quad \begin{pmatrix}0&1&1\\1&0&1\\1&1&0\end{pmatrix}$$



5. Ausblick

Im Hinblick auf die besondere Wichtigkeit primer Matrizen beim Erzeugen des Monoids $\mathbf{B}_n$ ergeben sich vielfältige Probleme. Dazu gehört das Finden einer hinreichenden und notwendigen Bedingung dafür, daß eine Matrix prim ist. Besonders zu erwähnen sind in diesem Zusammenhang die Ergebnisse von de Caen und Gregory [dCG80, dCG81], die sowohl hinreichende als auch notwendige Kriterien für prime Matrizen gefunden haben. Des weiteren wäre nicht nur ein Beweis dafür, daß die Anzahl der primen $\mathscr{D}$-Klassen exponentiell mit n wächst interessant, sondern auch die Beantwortung der Frage, wieviel prime $\mathscr{D}$-Klassen bzw. prime Matrizen es überhaupt gibt. Ungeklärt ist auch, welche Matrizen das Produkt primer Matrizen sind (Problem 5.3 in [dCG81]) und welche weder regulär erzeugt (also in $\mathbf{B}_n^r$ enthalten), noch prim sind. Meiner Meinung nach sind die primen Matrizen längst nicht so gut faßbar wie andere Matrizen.
Als Folgerung aus der Angabe der Erzeugendensysteme würde sich die Betrachtung einer Normalform für Matrizen anbieten, d.h. eine Darstellung jeder Matrix als Produkt von Elementen des Erzeugendensystems. Im Fall des Monoids $\mathbf{B}_n^r$ erfordert dies eine genauere Konstruktionsvorschrift im Beweis, da die Reihenfolge gewisser Operationen auf den Zeilen der Ausgangspermutation nicht festgelegt ist. Prinzipiell läßt sich aber jedes $\alpha \in \mathbf{B}_n^r$ als Produkt $\alpha = T_1 P T_2 \mu$ schreiben, wobei T_1, T_2 bzw. P ein Produkt von gewissen Matrizen des Typs t bzw. p ist und μ eine Permutation.
Der allgemeine Fall einer Matrix aus $\mathbf{B}_n$ ist schon aufgrund der primen Matrizen nicht so einfach handhabbar.
Weiterhin stellt sich die Frage nach einer Beschreibung der maximalen Untermonoide von $\mathbf{B}_n$. Dahingehend ist das Resultat von Montague und Plemmons [MP69] interessant, welches besagt, daß jede endliche Gruppe isomorph zu einer maximalen Untergruppe von $\underline{\mathbf{B}}_M$ ist. Dieses wurde von Schein [PS70] und Clifford [Cli70] sogar auf unendliche Gruppen übertragen (mit einer dann unendlichen Menge M).
Schlußendlich könnte die Übertragung einiger Resultate über binäre Relationen von Zarecki [Zar63] in die Sprache der formalen Begriffsanalyse zu weiteren Erkenntnissen führen.

Literatur

[Bir67] Garrett Birkhoff. *Lattice Theory*, volume XXV of *American Mathematical Society Colloqium Publications*. American Mathematical Society, Providence, Rhode Island, 3. edition, 1967.

[Cli70] A. H. Clifford. A proof of the Montague-Plemmons-Schein Theorem on maximal subgroups of the semigroup of binary relations. *Semigroup Forum*, 1:272–275, 1970.

[CP61] A. H. Clifford and G. B. Preston. *The Algebraic Theory of Semigroups, Volume I*. Number 7 in Mathematical Surveys. American Mathematical Society, Providence, Rhode Island, 1961.

[dCG80] D. de Caen and D. A. Gregory. Prime boolean matrices. In *Combinatorial Mathematics VII*, volume 829 of *Lecture Notes in Mathematics*, pages 76–82, 1980.

[dCG81] D. de Caen and D. A. Gregory. Primes in the semigroup of boolean matrices. *Linear Algebra and its Applications*, 37:119–134, 1981.

[Dev68] H. M. Devadze. Erzeugende Mengen der Halbgruppe aller binären Relationen auf einer endlichen Menge. *Doklady Akademii Nauk BSSR*, 12(9):765–768, 1968. (russisch).

[DKR76] J. Denes, K. H. Kim, and F. W. Roush. A characterization of an inverse for semigroup elements. Seminar report, Alabama State University, Montgomery, Alabama, 1976.

[Gre51] J. A. Green. On the structure of semigroups. *Annals of Math.*, 54:163–172, 1951.

[KHJ04] Daniela Kriegel, Andreas Hahn, and Robert Jäschke. Halbgruppen binärer Relationen auf einer 3-elementigen Menge. Seminararbeit, Technische Universität Dresden, 2004.

[Kim82] Ki Hang Kim. *Boolean Matrix Theory and Applications*, volume 70 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, New York, 1982.

[Kon92] Janusz Konieczny. *Semigroups of binary Relations*. PhD thesis, The Pennsylvania State University, University Park, PA, 1992.

[Kon94] Janusz Konieczny. Green's equivalences in finite semigroups of binary relations. *Semigroup Forum*, 48:235–252, 1994.

[Kon02] Janusz Konieczny. The semigroup generated by regular boolean matrices. *Southeast Asian Bulletin of Mathematics*, 25:627–641, 2002.

[Kon05] Janusz Konieczny. A proof of Devadze's theorem on generators of the semigroup of boolean matrices. 2005. to be published.

[KR77] Ki Hang Kim and Fred W. Roush. On generating regular elements in the semigroup of binary relations. *Semigroup Forum*, 14:29–32, 1977.

[KR78] Ki Hang Kim and Fred W. Roush. Inverses of boolean matrices. *Linear Algebra and its Applications*, 22:247–262, 1978.

[MP69] J. S. Montague and R. J. Plemmons. Maximal subgroups of the semigroup of relations. *Journal of Algebra*, 13:575–587, 1969.

[PS70] R. J. Plemmons and B. M. Schein. Groups of binary relations. *Semigroup Forum*, 1:267–271, 1970.

[PW70] R. J. Plemmons and M. T. West. On the semigroup of binary relations. *Pacific Journal of Mathematics*, 35(3):743–753, 1970.

[Sch76] Boris M. Schein. Regular elements of the semigroup of all binary relations. *Semigroup Forum*, 13:95–102, 1976.

[vN36] J. von Neumann. On regular rings. *Proceedings of the National Academy of Sciences of the United States of America*, 22:296–300, 1936.

[Yan69] Jaw-Ching Yang. A theorem on the semigroup of binary relations. *Proceedings of the American Mathematical Society*, 22:134–135, 1969.

[Zar63] K. A. Zarecki. Die Halbgruppe der binären Relationen. *Matematiceskij Sbornik*, 61:291–305, 1963. (russisch).

Erklärung

Hiermit erkläre ich, daß ich die am heutigen Tag eingereichte Diplomarbeit zum Thema „*Die Struktur der Monoide binärer Relationen auf endlichen Mengen*“ unter der Betreuung von Prof. Dr. Pöschel selbständig erarbeitet, verfasst und Zitate kenntlich gemacht habe. Andere als die angegebenen Hilfsmittel wurden von mir nicht benutzt.

Datum Unterschrift

Thesen zur Diplomarbeit

Die Struktur der Monoide binärer Relationen auf endlichen Mengen

vorgelegt von

Robert Jäschke

1. Alle binären Relationen auf einer Menge bilden zusammen mit dem Relationenprodukt ein Monoid, genannt *Monoid der binären Relationen*. Boolesche $(n \times n)$-Matrizen bieten sich als Darstellungsform dieser Relationen an und bilden mit einem geeigneten Matrizenprodukt ebenfalls ein Monoid, das *Monoid* $\mathbf{B}_n$ *der Booleschen* $(n \times n)$*-Matrizen*. Neben Verbindungen zur Theorie der Halbgruppen und Monoide gibt es auch Beziehungen zur Verbandstheorie und zur formalen Begriffsanalyse.

2. Ziel der vorliegenden Arbeit ist es, die Erzeugendensysteme für das Monoid $\mathbf{B}_n$ zu charakterisieren und die Struktur der Elemente der minimalen Erzeugendensysteme zu untersuchen. Des weiteren werden Untermonoide von $\mathbf{B}_n$ und deren Erzeugendensysteme betrachtet. Dazu gehören das Monoid aller Permutationsmatrizen $\mathbf{S}_n$, das von den regulären Elementen erzeugte Monoid $\mathbf{B}_n$ und ein Untermonoid, welches alle mageren Matrizen mit maximalem Zeilen- und Spaltenrang enthält.

3. Das im Jahre 1968 von H. M. Devadze ohne Beweis veröffentlichte Theorem über minimale Erzeugendensysteme für $\mathbf{B}_n$ wird bewiesen. Es besagt folgendes:

   > Sei $\mathfrak{M}$ ein minimales Erzeugendensystem für $\mathbf{S}_n$, π eine Matrix vom Typ p, τ eine Matrix vom Typ t, ϱ eine Matrix vom Typ r, ϱ' eine Matrix vom Typ r′ und $\mathfrak{P}$ eine Menge, die aus jeder primen $\mathscr{D}$-Klasse genau eine Matrix enthält. Dann sind die Mengen $\mathfrak{M} \cup \mathfrak{P} \cup \{\pi, \tau\}$ und $\mathfrak{M} \cup \mathfrak{P} \cup \{\varrho, \varrho', \tau\}$ minimale Erzeugendensysteme für $\mathbf{B}_n$ und in jedem Erzeugendensystem für $\mathbf{B}_n$ ist eine Menge von einer dieser beiden Arten enthalten.

4. Bestimmte Matrizen wurden von Devadze in *Typen* eingeteilt. Die Matrizen, die von einem dieser Typen sind, haben als einen ihrer Faktoren stets eine Matrix vom gleichen oder einem anderen Typ. Daraus folgern wir, daß jedes Erzeugendensystem für $\mathbf{B}_n$ Matrizen bestimmter Typen enthalten muß. Gleiches gilt für *prime* Matrizen, welche als Faktor stets eine zu sich selbst *äquivalente* Matrix enthalten.

5. Wir betrachten die Zeilen und Spalten einer Booleschen Matrix im Verband der Booleschen Vektoren und das von ihnen erzeugte Kernsystem (*Zeilenverband, Spaltenverband*) sowie die zugehörigen supremum-irreduziblen Elemente (*Zeilenbasis, Spaltenbasis*). Grundlegende Erkenntnisse über diese Begriffe bilden die Voraussetzung für Aussagen über *reguläre* und *prime* Matrizen sowie weitere wichtige Lemmata.