Teil 1. Verbände und Boolesche Algebren I. Verbände

Definition 0.1 *Es sei M eine nichtleere Menge und $\leq$ eine zweistellige Relation auf M. $\leq$ heißt* ***partielle Ordnung****, falls $\leq$ reflexiv, transitiv und antisymmetrisch ist. Dabei ist $\leq$* ***reflexiv*** *falls $x \leq x$ für alle $x \in M$,* ***transitiv*** *falls aus $x \leq y$ und $y \leq z$ schon $x \leq z$ folgt für alle $x, y, z \in M$, und $\leq$ heißt* ***antisymmetrisch****, falls aus $x \leq y$ und $y \leq x$ folgt $x = y$, für alle $x, y \in M$. Das Paar $\langle M, \leq \rangle$ heißt dann eine* ***partiell geordnete Menge*** *(Englisch* ***partially ordered set****, kurz* ***poset****). $\langle M, \leq \rangle$ und $\langle N, \leq' \rangle$ heißen* ***isomorph****, falls es eine Abbildung $g : M \to N$ gibt, welche bijektiv ist, und für die gilt $g(x) \leq' g(y)$ gdw. $x \leq y$, für alle $x, y \in M$. g heißt dann ein* ***Isomorphismus*** *von $\langle M, \leq \rangle$ auf $\langle N, \leq' \rangle$.*

Definition 0.2 *Es sei $\langle M, \leq \rangle$ eine partiell geordnete Menge und $X \subseteq M$. y heißt* ***obere Schranke von*** *X, falls $x \leq y$ für alle $x \in X$. y heißt* ***untere Schranke von*** *X, falls $y \leq x$ für alle $x \in X$. Falls ein eindeutig bestimmtes $y \in M$ existiert, sodaß $y \leq z$ gilt für jede obere Schranke z von X, so heißt y das* ***Supremum*** *von X, in Zeichen $\sup_{\leq} X$. Falls ein eindeutig bestimmtes u existiert, sodaß $z \leq u$ gilt jede untere Schranke z von X, so heißt u das* ***Infimum*** *von X, in Zeichen $\inf_{\leq} X$. Ist die Ordnung aus dem Kontext klar, schreiben wir auch $\inf X$ statt $\inf_{\leq} X$ und $\sup X$ statt $\sup_{\leq} X$. $\leq$ heißt eine* ***Verbandsordnung****, falls $\sup X$ und $\inf X$ existieren für alle endlichen $X \subseteq M$.*

Beispiele für Verbandsordnungen.

Beispiel 1. Es sei M die Menge aller natürlichen Zahlen mit der üblichen Ordnung $\leq$. Dies ist eine partielle Ordnung. Ferner ist $\inf X$ schlicht das Minimum aller Elemente aus X, $\sup X$ (für endliches X) stets das Maximum aller Elemente aus X. Wir sehen hier auch gleich, daß Suprema unendlicher Mengen nicht existieren müssen, selbst wenn Suprema aller endlichen Megen existieren; denn M hat kein Supremum. (Es gibt keine größte natürliche Zahl.)

Beispiel 2. Sei Q eine Menge. Dann ist $\subseteq$ eine Verbandsordnung auf $\wp(Q)$, der Potenzmenge von Q. Ist nämlich $X = \{P_1, P_2, \ldots, P_n\}$, so ist

$$\begin{aligned} \inf X &= P_1 \cap P_2 \cap \ldots \cap P_n \\ \sup X &= P_1 \cup P_2 \cup \ldots \cup P_n \end{aligned}$$

Beispiel 3. Es sei M wieder die Menge der natürlichen Zahlen. Diesmal betrachten wir die Ordnung $|$, die Teilbarkeitsrelation. $m \mid n$ bedeutet, daß m n teilt. Dies ist eine partielle Ordnung und $\inf X$ ist der ggT von X (größter gemeinsamer Teiler) und $\sup X$ das kgV von X (kleinstes gemeinsames Vielfaches).

Es ist klar, daß wenn $\langle P, \leq \rangle$ eine Verbandsordnung ist und $\langle Q, \leq' \rangle$ isomorph zu $\langle P, \leq \rangle$, so ist auch $\langle Q, \leq' \rangle$ eine Verbandsordnung.

Satz 0.3 *Genau dann ist $\leq$ eine Verbandsordnung auf M, falls Infima und Suprema von zweielementigen Mengen existieren. Ist nämlich $X = \{x_1, x_2, \ldots, x_n\}$,*

so

$$\begin{array}{rcl} supX & = & sup\{x_n, sup\{x_{n-1}, \ldots, sup\{x_2, x_1\} \ldots\}\} \\ infX & = & inf\{x_n, inf\{x_{n-1}, \ldots, inf\{x_2, x_1\} \ldots\}\} \end{array}$$

Beweis. Die Behauptung folgt mittels Induktion aus folgenden zwei Tatsachen: $sup\{x\} = x$ und $sup\{x, supY\} = sup\{x\} \cup Y$. Ersteres ist leicht zu sehen. Wir zeigen die zweite Behauptung. Sei $u \geq sup\{x, supY\}$. Dann ist $u \geq x$ und $x \geq supY$ und so für jedes $y \in Y$: $u \geq y$. Daraus folgt sofort $u \geq z$ für jedes $z \in \{x\} \cup Y$, also $u \geq sup\{x\} \cup Y$. Nun sei umgekehrt $u \geq sup\{x\} \cup Y$. Dann ist $u \geq y$ für jedes $y \in Y$, also $u \geq supY$. Da auch $u \geq x$, so ist $u \geq sup\{x, supY\}$. Dies zeigt, daß $sup\{x, supY\} = sup\{x\} \cup Y$. Analog für Infima. Q. E. D.

Satz 0.4 *Es gelten folgende Gesetze*

$$\begin{array}{rclrcl} sup\{x, sup\{y, z\}\} & = & sup\{sup\{x, y\}, z\} & inf\{x, inf\{y, z\}\} & = & inf\{inf\{x, y\}, z\} \\ sup\{x, x\} & = & x & inf\{x, x\} & = & x \\ sup\{x, inf\{x, y\}\} & = & x & inf\{x, sup\{x, y\}\} & = & x \end{array}$$

Beweis. Aus dem vorigen Satz folgt $sup\{x, sup\{y, z\}\} = sup\{x, y, z\}$ sowie $sup\{z, sup\{x, y\}\} = sup\{x, y, z\}$, und so ist das erste Gesetz bewiesen. Ebenso das zweite Gesetz. Gewiß ist $sup\{x, x\} = sup\{x\} = x$ und $inf\{x, x\} = inf\{x\} = x$. Die letzten beiden Gesetze sieht man so. Es ist $x \geq inf\{x, y\}$. Also ist $sup\{x, inf\{x, y\}\} = x$. Ferner ist $x \leq sup\{x, y\}$ und so $x = inf\{x, sup\{x, y\}\}$. Q. E. D.

Satz 0.5 (Dualitätsprinzip) *Es sei $\mathfrak{M} = \langle M, \leq \rangle$ eine partielle Ordnung. Dann ist auch $\mathfrak{M}^{op} := \langle M, \geq \rangle$ eine partielle Ordnung. Wir nennen $\mathfrak{M}^{op}$ die zu $\mathfrak{M}$* ***duale Ordnung****. Ist ferner $\leq$ eine Verbandsordnung auf M, so auch $\geq$. Ferner ist*

$$\begin{array}{rcl} inf_{\geq} X & = & sup_{\leq} X \\ sup_{\geq} X & = & inf_{\leq} X \end{array}$$

Beweis. Ist $x \leq x$ für alle x, so auch $x \geq x$. Ist $x \geq y$ und $y \geq z$, so $z \leq y$ und $y \leq x$, also $z \leq x$, was nichts anderes ist als $x \geq z$. Endlich sei $x \geq y$ und $y \geq x$. Dann $x \leq y$ und $y \leq x$, und so $x = y$. Nun zum zweiten Teil. Es sei $\leq$ eine Verbandsordnung. Sei ferner X eine endliche Teilmenge von M. Dann existiert $z := sup_{\leq} X$. Es sei $u \geq x$ für alle $x \in X$. Dann $x \leq u$ für alle $x \in X$. Daraus folgt $z \leq u$. Also $u \geq z$. Dies bedeutet $z = inf_{\geq} X$. Analog zeigt man das zweite Gesetz. Q. E. D.

Definition 0.6 *Es sei V eine nichtleere Menge und $\sqcap$ und $\sqcup$ zweistellige Operationen auf V. Das Tripel $\langle V, \sqcap, \sqcup \rangle$ heißt* ***Verband****, falls folgende Gesetze gelten für alle $x, y, z \in V$.*

$$\begin{array}{rclrcl} x \sqcap (y \sqcap z) & = & (x \sqcap y) \sqcap z & x \sqcup (y \sqcup z) & = & (x \sqcup y) \sqcup z \\ x \sqcap y & = & y \sqcap x & x \sqcup y & = & y \sqcup x \\ x \sqcap x & = & x & x \sqcup x & = & x \\ x \sqcap (y \sqcup x) & = & x & x \sqcup (y \sqcap x) & = & x \end{array}$$

Satz 0.7 *(1.) Es sei $\leq$ eine Verbandsordnung auf M. Setze $x \sqcup y := sup_{\leq}\{x, y\}$ und $x \sqcap y := inf_{\leq}\{x, y\}$. Dann ist $\langle M, \sqcap, \sqcup\rangle$ ein Verband. (2.) Es sei $\langle V, \sqcap, \sqcup\rangle$ ein Verband. Setze $x \leq y \Leftrightarrow x \sqcap y = x$. Dann ist $x \leq y$ genau dann, wenn $x \sqcup y = y$, und $\leq$ ist eine Verbandsordnung auf V. Ferner ist $sup_{\leq}\{x, y\} = x \sqcup y$ und $inf_{\leq}\{x, y\} = x \sqcap y$.*

Beweis. Der erste Teil ist klar wegen Satz 0.4. Nun zum zweiten Teil. Sei $x \sqcap y = x$. Dann ist $x \sqcup y = (x \sqcap y) \sqcup y = y \sqcup (x \sqcap y) = y$. Ebenso, ist $x \sqcup y = y$, dann ist $x \sqcap y = x \sqcap (x \sqcup y) = x \sqcap (y \sqcup x) = x$. Daß $\leq$ eine Verbandsordnung ist, sieht man so. Da $x \sqcap x = x$, ist $x \leq x$. Ferner, sei $x \leq y$ und $y \leq z$. Dann ist $x \sqcap y = x$ und $y \sqcap z = y$. Daraus folgt $x \sqcap z = (x \sqcap y) \sqcap z = x \sqcap (y \sqcap z) = x \sqcap y = x$. Also $x \leq z$. Schließlich sei $x \leq y$ und $y \leq x$. Dann isr $x \sqcap y = x$ und $y \sqcap x = y$. Aber $x \sqcap y = y \sqcap x$; also $x = y$. Also ist $\leq$ eine partielle Ordnung. Es bleibt zu zeigen, daß $\leq$ eine Verbandsordnung ist. Es genügt, die Existenz von Suprema und Infima zweielementiger Mengen nachzuweisen. Wir behaupten nun, daß $inf_{\leq}\{x, y\} = x \sqcap y$ ist und $sup_{\leq}\{x, y\} = x \sqcup y$. Sei nämlich $z \geq x$ und $z \geq y$, also $x \sqcup z = z$ sowie $y \sqcup z = z$. Dann ist $x \sqcup y \leq z$, denn $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z) = x \sqcup z = z$. Q. E. D.

Es besteht also eine eineindeutige Korrespondenz zwischen Verbandsordnungen und Verbänden. Man mache sich dies anhand der Beispiele 1 – 3 klar. Wir machen darauf aufmerksam, daß folgendes gilt.

$$\begin{array}{lll} x \geq (y \sqcup z) & \text{gdw.} & x \geq y \text{ und } x \geq z \\ x \leq (y \sqcap z) & \text{gdw.} & x \leq y \text{ und } x \leq z \end{array}$$

Ferner ist $x \leq x \sqcup y$ und $x \geq x \sqcap y$, wie man leicht sieht. Auch nützlich ist folgendes Gesetz. Ist $x \leq y$, so $x \sqcup z \leq y \sqcup z$ und $x \sqcap z \leq y \sqcap z$. Nämlich, aus $x \leq y$ folgt $x \leq y \sqcup z$. Ferner ist ja $z \leq y \sqcup z$. Also $x \sqcup z \leq y \sqcup z$. Analog zeigt man, daß aus $x \leq y$ folgt $x \sqcap z \leq y \sqcap z$.

Satz 0.8 (Dualitätsprinzip) *Es sei $\mathfrak{V} = \langle V, \sqcap, \sqcup\rangle$ ein Verband. Dann ist auch $\mathfrak{V}^{op} := \langle V, \sqcup, \sqcap\rangle$ ein Verband. Wir nennen $\mathfrak{V}^{op}$ den zu $\mathfrak{V}$* ***dualen Verband****. Die Ordnung zu $\mathfrak{V}^{op}$ ist die Duale Ordnung zu der Ordnung von $\mathfrak{V}$.*

Das Dualitätprinzip kann man wie folgt ausbeuten. Sei α eine Aussage über Verbände. Es gehe α^{op} aus α durch Austauschen von $\sqcap$ und $\sqcup$, sowie $\leq$ und $\geq$ hervor. Dann ist α^{op} in allen Verbänden gültig genau dann wenn α in allen Verbänden gültig ist. Wir werden allerdings nicht näher präzisieren, was eine Aussage über Verbände ist. Dies sei eine jede sinvolle Aussage, welche außer logischen Symbolen noch $\sqcap$, $\sqcup$, $\leq$ und $\geq$ gebraucht. Zum Beweis muß man sich nur klarmachen, daß man eben (dank der Dualität) $\sqcap$ wahlweise auch als $\sqcup$ interpretieren darf, nur muß dann $\sqcup$ als $\sqcap$ und $\leq$ als $\geq$ interpretiert werden. Wir geben ein Beispiel. Die Aussage

$$(\forall xyz)((x \sqcap y) \sqcup (x \sqcap z) \leq x \sqcap (y \sqcup z))$$

ist in allen Verbänden gültig. Daher ist auch die Aussage

$$(\forall xyz)((x \sqcup y) \sqcap (x \sqcup z) \geq x \sqcup (y \sqcap z))$$

in allen Verbänden gültig.

Definition 0.9 *Es seien* $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ *und* $\mathfrak{W} = \langle W, \sqcap', \sqcup' \rangle$ *Verbände, und* $h : V \to W$ *eine beliebige Abbildung.* h *heißt* ***Homomorphismus*** *von* $\mathfrak{V}$ *nach* $\mathfrak{W}$*, in Zeichen* $h : \mathfrak{V} \to \mathfrak{W}$*, falls für alle* $x, y \in V$ *gilt*

$$\begin{array}{rcl} h(x \sqcap y) & = & h(x) \sqcap' h(y) \\ h(x \sqcup y) & = & h(x) \sqcup' h(y) \end{array}$$

h *heißt* ***Isomorphismus****, falls* h *bijektiv ist.* h *heißt* ***Endomorphismus****, falls* $\mathfrak{V} = \mathfrak{W}$*, und* ***Automorphismus****, falls* h *sowohl Endomorphismus ist wie auch Isomorphismus.*

Wir merken folgen Tatsache an.

Satz 0.10 *Es seien* $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ *und* $\mathfrak{W} = \langle W, \sqcap', \sqcup' \rangle$ *Verbände und* $h : V \to W$*. Genau dann ist* h *ein Isomorphismus, wenn* h *ein Isomorphismus von* $\langle V, \leq \rangle$ *auf* $\langle W, \leq' \rangle$ *ist.* $\mathfrak{V}$ *ist genau dann zu* $\mathfrak{W}$ *isomorph, wenn* $\langle V, \leq \rangle$ *zu* $\langle W, \leq' \rangle$ *isomorph ist.*

Daher stellt man einen konkreten Verband niemals in Form von Operationstafeln dar. Dies ist im allgemeinen nämlich unübersichtlich. Stattdessen gibt man den Ordnungstyp des Verbands an.

Übungen.

Übung 1. Es sei M eine Menge und $\Pi \subseteq \wp(M)$. Π heißt **Partition** von M, falls (i) $\emptyset \notin \Pi$, (ii) für $S, T \in \Pi$ und $S \neq T$ gilt $S \cap T = \emptyset$, (iii) die Vereinigung aller Mengen aus Π ist M. (Beispiel. $\{\{a\}, \{b, d\}, \{c, e, f\}\}$ ist eine Partition der Menge $\{a, b, c, d, e, f\}$.) Π heißt **feiner** als Σ, falls zu jeder Menge $S \in \Pi$ eine Menge $T \in \Sigma$ existiert mit $S \subseteq T$. Sei $\Pi \leq \Sigma$ falls Π feiner ist als Σ. Sei $\Pi(M)$ die Menge aller Partitionen auf M. Diese sind durch $\leq$ partiell geordnet. (Dies müssen Sie hier nicht zeigen.) Zeichnen Sie $\langle \Pi(M), \leq \rangle$ für $M = \{1, 2, 3, 4\}$.

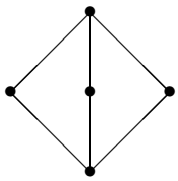
Übung 2. Eine zweistellige Relation $\sim$ heißt **symmetrisch**, falls aus $x \sim y$ folgt $y \sim x$ für alle $x, y \in M$. $\sim$ heißt **Äquivalenzrelation**, falls $\sim$ reflexiv, symmetrisch und transitiv ist. Sei $A(M)$ die Menge der Äquivalenzrelationen auf M. Zeigen Sie: $\langle \Pi(M), \leq \rangle$ ist isomorph zu $\langle A(M), \subseteq \rangle$. Zeigen Sie so, daß $\langle \Pi(M), \leq \rangle$ eine partiell geordnete Menge ist. (Wer Lust hat, möge zeigen, daß $\langle \Pi(M), \leq \rangle$ ein Verband ist und die zugehörigen Operationen bestimmen. Es winken Extrapunkte.) *Hinweis.* Ist Π eine Partition, setze $x \sim_\Pi y$ gdw. ein $T \in \Pi$ existiert mit $x, y \in T$. Ist umgekehrt $\approx$ eine Äquivalenzrelation, so sei $[x] = \{y : x \approx y\}$ und $\Pi_\approx := \{[x] : x \in M\}$.

Übung 3. Es sei $\leq$ eine partielle Ordnung auf M. $\leq$ heißt **linear**, falls für je zwei Elemente $x, y \in M$ gilt $x \leq y$ oder $y \leq x$. Zeigen Sie: eine lineare partielle Ordnung ist eine Verbandsordnung.

Übung 4. Zeigen Sie, daß in allen Verbänden gilt

$$(\forall xyz)((x \sqcap y) \sqcup (x \sqcap z) \leq x \sqcap (y \sqcup z))$$

Übung 5. Bestimmen Sie alle Automorphismen des folgenden Verbandes.



Teil 2. Verbände und Boolesche Algebren II. Distributive Verbände

Ein Element x eines Verbandes $\langle V, \sqcap, \sqcup \rangle$ heißt ein **minimales Element** oder eine **Null**, falls $x \leq y$ für alle $y \in V$. x heißt ein **maximales Element** oder eine **Eins**, falls $x \geq y$ für alle $y \in V$. Es muß weder eine Null noch eine Eins geben; falls es sie gibt, sind sie jeweils eindeutig bestimmt. Man notiert die Null mit 0 oder $\perp$, die Eins mit 1 oder $\top$. Es gilt stets $x \sqcap 1 = x$ und $x \sqcup 0 = x$. Ist X eine beliebige endliche Teilmenge von V, so sei $\bigsqcap X := \mathit{inf}\, X$ und $\bigsqcup X := \mathit{sup} X$. Es ist leicht zu sehen, daß in einem endlichen Verband $\bigsqcap V$ eine Null und $\bigsqcup V$ eine Eins ist. Hat $\mathfrak{V}$ eine Eins, so setze $\mathit{inf}\emptyset := 1$; hat $\mathfrak{V}$ eine Null, so setze $\mathit{sup}\emptyset := 0$.

Definition 0.11 *Ein Verband heißt* ***distributiv****, falls für alle $x, y, z \in V$ gilt*

$$\begin{array}{rcl} x \sqcap (y \sqcup z) & = & (x \sqcap y) \sqcup (x \sqcap z) \\ x \sqcup (y \sqcap z) & = & (x \sqcup y) \sqcap (x \sqcup z) \end{array}$$

Man kann zeigen, daß jeweils eine der beiden Forderungen die andere impliziert. Wir wollen dies nicht tun. Wir geben stattdessen ein allgemeines Verfahren an, wie man distributive Verbände basteln kann und zeigen anschließend, daß man über dieses Verfahren zumindest alle endlichen distributiven Verbände bekommt.

Beispiel 1. Es sei X eine Menge, und $\wp(X)$ die Potenzmenge von X. Dann ist $\langle \wp(X), \cap, \cup \rangle$ eine distributiver Verband. $\varnothing$ ist darin eine Null, X eine Eins. Wir nennen dies den **Teilerverband** von n.

Beispiel 2. Es sei n eine natürliche Zahl, und $T(n)$ die Menge der Teiler von n. Dann ist $\langle T(n), ggT, kgV \rangle$ ein distributiver Verband, mit 1 als Null (!) und n als Eins. Man beachte, daß $x \leq y$ gilt gdw. x ein Teiler von y ist.

Beispiel 3. Es sei $\mathfrak{P} = \langle P, \leq \rangle$ eine partiell geordnete Menge. Ist $S \subseteq P$, so setze

$$\begin{array}{rcl} \downarrow S & := & \{y : (\exists x \in S)(y \leq x)\} \\ \uparrow S & := & \{y : (\exists x \in S)(y \geq x)\} \end{array}$$

Ist $S = \downarrow S$, so heißt S **nach unten abgeschlossen**. Mit anderen Worten, ist $S = \downarrow S$, so folgt aus $x \in S$ und $y \leq x$, daß auch $y \in S$ ist. Man kann nun leicht

zeigen, daß der Schnitt und die Vereinigung zweier nach unten abgeschlossener Mengen wieder nach unten abgeschlossen ist. Seien nämlich S und T nach unten abgeschlossen, $x \in S \cap T$ und $y \leq x$. Dann $x \in S$, und so $y \in S$, und es ist $x \in T$ und so $y \in T$. Ferner, falls $x \in S \cup T$, etwa $x \in S$, und $y \leq x$, so ist $y \in S$, also $y \in S \cup T$. Analog falls $x \in T$. Sei $L(\mathfrak{P})$ die Menge der nach unten abgeschlossenen Mengen. Dann ist $\mathfrak{Vb}(\mathfrak{P}) := \langle L(\mathfrak{P}), \cap, \cup \rangle$ ein distributiver Verband.

Definition 0.12 *Es sei $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ ein Verband. $x \in V$ heißt $\sqcup$–**irreduzibel** oder schlicht **irreduzibel**, falls x nicht $\leq$–minimal und aus $x = y \sqcup z$ folgt $x = y$ oder $x = z$. Dual heißt x $\sqcap$–**irreduzibel**, falls x nicht $\leq$–maximal und aus $x = y \sqcap z$ folgt $x = y$ oder $x = z$.*

Zum Beispiel ist in dem Teilerverband von n eine Zahl irreduzibel, falls sie die Potenz einer Primzahl ist. Denn sei $k = p^m$ für eine Primzahl p und eine natürliche Zahl m. Ist k ein Teiler von $kgV\{x, y\}$, so muß k entweder x oder y teilen. Ist aber $k = p^m \cdot y$ für ein $y \neq 1$, welches nicht durch p teilbar ist, so ist $k = kgV\{p^m, y\}$, aber es ist k kein Teiler von p^m oder y. Also ist k nicht irreduzibel.

Es sei $\mathfrak{V}$ ein endlicher Verband. Sei $Irr(\mathfrak{V})$ die Menge der Irreduziblen Elemente von $\mathfrak{V}$. $\langle Irr(\mathfrak{V}), \leq \rangle$ ist eine partiell geordnete Menge. Setze $\zeta(x) := \{y \in Irr(\mathfrak{V}) : y \leq x\}$. Dann ist $\zeta(x)$ eine nach unten abgeschlossene Menge in $\langle Irr(\mathfrak{V}), \leq \rangle$.

Hilfssatz 0.13 *Es sei $\mathfrak{V}$ ein distributiver Verband. Dann gilt*

$$\begin{aligned} \zeta(x \sqcup y) &= \zeta(x) \cup \zeta(y) \\ \zeta(x \sqcap y) &= \zeta(x) \cap \zeta(y) \end{aligned}$$

Beweis. Es sei $u \in \zeta(x \sqcup y)$. Dann ist u irreduzibel und $u \leq x \sqcup y$. Daraus folgt $u = u \sqcap (x \sqcup y) = (u \sqcap x) \sqcup (u \sqcap y)$, also ist $u = u \sqcap x$ oder $u = u \sqcap y$. Daher ist $u \leq x$ oder $u \leq y$. Nach Definition heißt dies, daß $u \in \zeta(x)$ oder $u \in \zeta(y)$. Sei nun $u \in \zeta(x)$ oder $u \in \zeta(y)$. Dann $u \leq x$ oder $u \leq y$, und so $u \leq x \sqcup y$. u ist irreduzibel, also $u \in \zeta(x \sqcup y)$. Nun zur zweiten Behauptung. Sei $u \in \zeta(x \sqcap y)$, also $u \leq x \sqcap y$ und u irreduzibel. Dann $u \leq x$ und $u \leq y$ und so $u \in \zeta(x)$ sowie $u \in \zeta(y)$. Ist umgekehrt $u \in \zeta(x)$ und $u \in \zeta(y)$, so $u \leq x$ und $u \leq y$, woraus $u \leq x \sqcap y$ folgt und schließlich $u \in \zeta(x \sqcap y)$. Q. E. D.

Wir haben damit gezeigt, daß $x \mapsto \zeta(x)$ ein Homomorphismus ist. Nun wollen wir noch zeigen, daß es eine bijektive Abbildung ist. Dazu sei zunächst M eine nach unten abgeschlossene Menge.

Hilfssatz 0.14 *Es sei M eine nach unten abgeschlossene Menge von irreduziblen Elementen in einem distributiven Verband. Dann gilt $M = \zeta(\bigsqcup M)$.*

Beweis. Mit anderen Worten: für ein irreduzibles Element u ist $u \leq \bigsqcup M$ genau dann, wenn $u \in M$. Falls $u \in M$, so ist sicher $u \leq \bigsqcup M$. Sei daher $u \leq \bigsqcup M$. Dann ist $u = u \sqcap \bigsqcup M = \bigsqcup \langle u \sqcap y : y \in M \rangle$. Da u irreduzibel, ist $u = u \sqcap y$ für ein $y \in M$, also $u \leq y$. Nun ist M nach unten abgeschlossen und u irreduzibel. Also $u \in M$. Q. E. D.

Hilfssatz 0.15 *Es sei $\mathfrak{V}$ ein endlicher Verband. Dann existiert für jedes $x \in V$ eine nach unten abgeschlossene Menge M aus $\sqcup$–irreduziblen Elementen, sodaß $x = \bigsqcup M$ ist. Diese Menge ist eindeutig, und $M = \zeta(x)$.*

Beweis. Zunächst zeigen wir die Eindeutigkeit. Sei $x = \bigsqcup M = \bigsqcup N$, wo M und N nach unten abgeschlossene Menge irreduzibler Elemente sind. Sei $u \in M$. Dann gilt $u \leq x$, und so $u \leq \bigsqcup N$. Also $u = u \sqcap (\bigsqcup N) = \bigsqcup_{y \in N}(u \sqcap y)$. Da u irreduzibel, existiert ein $y \in N$ mit $u = u \sqcap y$; daraus folgt $u \leq y$. Da N nach unten abgeschlossen ist, ist $u \in N$. Daher $M \subseteq N$. Ebenso zeigt man $N \subseteq M$. Nun zeigen wir, daß $x = \bigsqcup \zeta(x)$. Falls dies nicht der Fall ist, so ist $x > \bigsqcup \zeta(x)$. Sei y ein minimales Element mit der Eigenschaft, daß $y \nleq \bigsqcup \zeta(x)$, aber $y \leq x$. Solch ein Element muß es geben. Denn x hat diese Eigenschaft. Die Menge der Elemente mit dieser Eigenschaft ist also nichtleer und endlich. Dann hat sie ein kleinstes Element. Wir zeigen, daß y irreduzibel ist, woraus folgt $y \in \zeta(x)$, im Gegensatz zu unserer Annahme. Sei also $y = z_1 \sqcup z_2$. Dann ist $z_1 \nleq \zeta(x)$ oder $z_2 \nleq \zeta(x)$. Sei etwa $z_1 \nleq \zeta(x)$. Sicher ist $z_1 \leq x$. Nach Wahl von y ist also $z_1 = y$. Also ist y irreduzibel. Q. E. D.

Es läßt sich zeigen, daß die Eindeutigkeit der Zerlegung ein Kriterium dafür ist, ob der Verband distributiv ist oder nicht. Denn sei $x = \bigsqcup M = \bigsqcup N$ für zwei verschiedene, nach unten abgeschlossene Mengen. Dann existiert oBdA ein $u \in M - N$. Also ist $u < \bigsqcup N$. Man kann leicht sehen, daß N kein maximales Element enthält. (Denn dann ist x schon irreduzibel und dann muß $x \in M$ sein, woraus sogleich $N \subseteq M$ folgt. Aber $N \subsetneq M$ kann nicht sein, denn daraus folgt $\bigsqcup N < \bigsqcup M$.) Also ist $N = S_1 \cup S_2$, wo S_1 und S_2 jeweils nicht leer sind. Wir können sogar annehmen, daß S_1 und S_2 nach unten abgeschlossen sind. Setze $y := \bigsqcup S_1$ und $z := \bigsqcup S_2$. Dann ist

$$u \sqcap (y \sqcup z) = u \sqcap x = u$$

Angenommen,

$$(u \sqcap y) \sqcup (u \sqcup z) = u$$

Dann ist $u \sqcap y = u$ oder $u \sqcap z = u$, da u irreduzibel. Sei etwa $u \sqcap y = u$. Dann $u \in S_1$, da S_1 nach unten abgeschlossen und u irreduzibel. Dies widerspricht der Annahme, daß $y \notin N$.

Als Anwendung betrachten wir noch einmal den Teilerverband von n. Ein beliebiges Element ist eindeutig darstellbar als das kgV einer bezüglich Teilbarkeit nach unten abgeschlossenen Menge von Primzahlpotenzen. Daraus folgt unmittelbar die Eindeutigkeit der Zerlegung in Primfaktoren.

Satz 0.16 (Darstellungssatz für endliche Distributive Verbände) *Es sei $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ ein endlicher distributiver Verband, $\mathfrak{P} = \langle Irr(\mathfrak{V}), \leq \rangle$ die partielle Ordnung der $\sqcup$–irreduziblen Elemente. Dann ist $\mathfrak{V}$ isomorph zu $\mathfrak{Vb}(\mathfrak{P}) := \langle L(\mathfrak{P}), \cap, \cup \rangle$.*

Beweis. Betrachte $x \mapsto \zeta(x)$. Diese Abbildung ist ein Homomorphismus (Hilfssatz 0.13). ζ ist surjektiv wegen Hilfssatz 0.14 und injektiv wegen Hilfssatz 0.15. Q. E. D.

Man beachte, daß man die Distributivität im Wesentlichen für die Eindeutigkeit der Zerlegung braucht. Es ist nämlich in allen endlichen Verbänden jedes Element die Vereinigung irreduzibler Elemente, aber da diese Darstellung nicht eindeutig ist, kann man daraus keinen Isomorphismus konstruieren (sonst wäre ja auch jeder endliche Verband distributiv — und das ist nicht der Fall).

Sei x ein Element und y derart, daß $y < x$ aber kein z existiert mit $y < z < x$. Dann sagen wir, y sei ein **unterer Nachbar** von x und x sei **oberer Nachbar** von y und schreiben $y \prec x$. Wir folgern aus dem Darstellungssatz für distributive Verbände ein handliches Kriterium.

Hilfssatz 0.17 *Es sei $\mathfrak{V}$ ein endlicher distributiver Verband. Dann ist $u \leq v$ genau dann, wenn $\zeta(u) \subseteq \zeta(v)$. Ferner ist $u \prec v$ genau dann, wenn $\zeta(v) = \zeta(u) \cup \{x\}$ ist für ein irreduzibles x, welches nicht in $\zeta(u)$ ist.*

Beweis. Ist $u \leq v$, so ist jedes Element unterhalb von u auch unterhalb von v, also $\zeta(u) \subseteq \zeta(v)$. Ist umgekehrt $\zeta(u) \subseteq \zeta(v)$, so ist $u = \bigsqcup \zeta(u) \leq \bigsqcup \zeta(v) = v$. Nun sei $\zeta(v) = \zeta(u) \cup \{x\}$ für ein $x \notin \zeta(u)$. Dann ist gewiß $u < v$. Falls ein z existiert mit $u < z < v$, so ist $\zeta(u) \subsetneq \zeta(z) \subsetneq \zeta(v)$. Dies ist nicht möglich. Also $u \prec v$. Sei umgekehrt $u \prec v$. Dann ist sicher $\zeta(u) \subsetneq \zeta(v)$. Sei x minimal bezüglich $\leq$ in der Menge $\zeta(v) - \zeta(u)$. Dann ist $\zeta(u) \cup \{x\}$ nach unten abgeschlossen. Denn ist $p \leq r \in \zeta(u) \cup \{x\}$ ein irreduzibles Element, so entweder $r \in \zeta(u)$ oder $r = x$. Im ersten Fall ist $r \in \zeta(u)$, da letztere Menge nach unten abgeschlossen ist. Im zweiten Fall ist entweder $p < x$ und damit $p \in \zeta(u)$, da x minimal war und $\zeta(u)$ nach unten abgeschlossen. Oder aber $x = p$, und so $x \in \zeta(u) \cup \{x\}$. Wir haben also $\zeta(u) \subsetneq \zeta(u) \cup \{x\} \subseteq \zeta(v)$. Da $u \prec v$, gilt $\zeta(v) = \zeta(u) \cup \{x\}$. Q. E. D.

Definition 0.18 *Es sei $\mathfrak{V}$ ein Verband. Eine Folge $F = \langle x_i : 0 \leq i \leq n \rangle$ heißt* **Kette***, falls für alle $i < m$, x_i unterer Nachbar von x_{i+1}. Darüber hinaus heißt F auch* **Kette von** x_0 **nach** x_n*. Sei x ein Element und n die größte Zahl — sofern sie existiert — derart, daß eine Kette $\langle y_i : 0 \leq i \leq n \rangle$ existiert mit $y_0 = 0$, $y_n = x$. Dann sagt man, x hat die* ***Dimension*** *n.*

Satz 0.19 *Es sei $\mathfrak{V}$ ein distributiver Verband, $x \in V$ ein Element mit Dimension n. Sei $\langle y_i : 0 \leq i \leq m \rangle$ eine beliebige Kette mit $y_0 = 0$, $y_m = x$. Dann ist $m = n$.*

Der Beweis für diesen Satz ist eine Übung. Man sagt, ein Verband ist **kettengleich**, falls für je zwei Elemente x, y gilt: existiert eine Kette von x nach y der Länge n, so hat jede Kette von x nach y die Länge n. Mit Hilfssatz 0.17 folgt jetzt leicht:

Hilfssatz 0.20 *Es sei $\mathfrak{V}$ ein endlicher distributiver Verband. Dann gilt für alle $x \in V$:*

$$dim x = \sharp \zeta(x) \ .$$

Ist $\mathfrak{V}$ ein Verband, so schreiben wir $[x, y] := \{z : x \leq z \leq y\}$ und nennen dies ein **Intervall**. Intervalle sind abgeschlossen unter $\sqcup$ und $\sqcap$ und bilden somit wiederum Verbände.

Satz 0.21 *Es sei $\mathfrak{V}$ ein distributiver Verband, und x, y beliebige Elemente. Dann ist das Intervall $[x \sqcap y, x]$ isomorph zu dem Intervall $[y, x \sqcup y]$. Ein Isomorphismus ist gegeben durch die Abbildung $h : z \mapsto z \sqcup y$.*

Beweis. Betrachte die Abbildung $k : z \mapsto z \sqcap x$. Wir behaupten: $k \circ h$ ist die Identität auf $[x \sqcap y, x]$ und $h \circ k$ die Identität auf $[y, x \sqcup y]$. Dazu sei $x \sqcap y \leq z \leq x$. Dann ist $(k \circ h)(z) = (z \sqcup y) \sqcap x = (z \sqcap x) \sqcup (y \sqcap x) = z \sqcup (x \sqcap y) = z$. Sei jetzt $y \leq u \leq x \sqcup y$. Dann $(h \circ k)(u) = (u \sqcap x) \sqcup y = (u \sqcup y) \sqcap (x \sqcup y) = u \sqcap (x \sqcup y) = u$. k und h sind ordnungstreu, das heißt, ist $z \leq z'$ für $z, z' \in [x \sqcap y, x]$, so $h(z) \leq h(z')$ und ist $u, u' \in [y, x \sqcup y]$, so folgt aus $u \leq u'$ bereits $k(u) \leq k(u')$. Ist nun $h(z) \leq h(z')$, so ist $(k \circ h)(z) \leq (k \circ h)(z')$, also $z \leq z'$. Ist $k(u) \leq k(u')$, so ist $(h \circ k)(u) \leq (h \circ k)(u')$, also $u \leq u'$. k und h sind also Ordnungsisomorphismen, und daher Verbandsisomorphismen. Q. E. D.

Als letztes besprechen wir noch eine wichtige Konstruktion in der Algebra, nämlich das **Produkt**. Das Produkt zweier Verbände wird wie folgt definiert. (Wir setzen nicht voraus, daß die Verbände distributiv sind.) Seien $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ und $\mathfrak{W} = \langle W, \sqcap', \sqcup' \rangle$ Verbände. Seien $\langle x_1, y_1 \rangle, \langle x_2, y_2 \rangle \in V \times W$. Dann setze

$$\begin{array}{rcl} \langle x_1, y_1 \rangle \sqcap'' \langle x_2, y_2 \rangle & := & \langle x_1 \sqcap x_2, y_1 \sqcap' y_2 \rangle \\ \langle x_1, y_1 \rangle \sqcup'' \langle x_2, y_2 \rangle & := & \langle x_1 \sqcup x_2, y_1 \sqcup' y_2 \rangle \end{array}$$

$\mathfrak{V} \times \mathfrak{W} := \langle V \times W, \sqcap'', \sqcup'' \rangle$ ist ein Verband. Dies nachzurechnen, ist langwierig, aber nicht schwer. Wir beweisen anstelle dessen folgenden Sachverhalt.

Hilfssatz 0.22 *Es seien $\mathfrak{V}$ und $\mathfrak{W}$ distributive Verbände. Dann ist $\mathfrak{V} \times \mathfrak{W}$ auch ein distributiver Verband.*

Beweis. Wir zeigen nur eines der beiden Gesetze (das andere ist ja dual dazu).

$$\begin{array}{rcl} \langle x_1, y_1 \rangle \sqcap'' (\langle x_2, y_2 \rangle \sqcup'' \langle x_3, y_3 \rangle) & = & \langle x_1, y_1 \rangle \sqcap'' \langle x_2 \sqcup x_3, y_2 \sqcup' y_3 \rangle \\ & = & \langle x_1 \sqcap (x_2 \sqcup x_3), y_1 \sqcap' (y_2 \sqcup' y_3) \rangle \\ & = & \langle (x_1 \sqcap x_2) \sqcup (x_1 \sqcap x_3), (y_1 \sqcap' y_2) \sqcup' (y_1 \sqcap' y_3) \rangle \\ & = & \langle x_1 \sqcap x_2, y_1 \sqcap' y_2 \rangle \sqcup'' \langle x_1 \sqcap x_3, y_1 \sqcap y_3 \rangle \\ & = & (\langle x_1, y_1 \rangle \sqcap'' \langle x_2, y_2 \rangle) \sqcup'' (\langle x_1, y_1 \rangle \sqcap'' \langle x_3, y_3 \rangle) \end{array}$$

Q. E. D.

Übungen

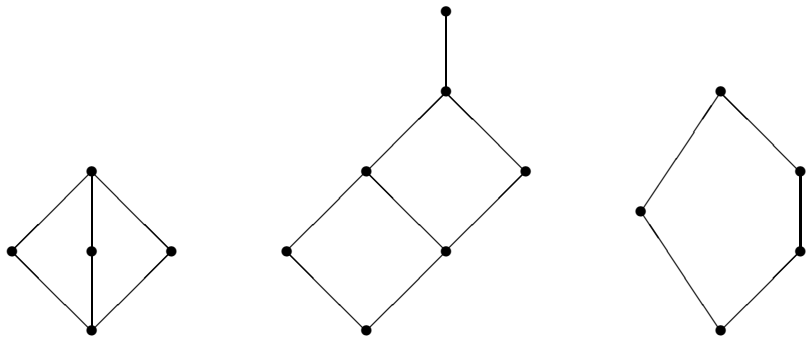
Übung 6. Seien $\mathfrak{P} = \langle P, \leq \rangle$ und $\mathfrak{Q} = \langle Q, \leq \rangle$ Ordnungen irreduzibler Elemente von $\mathfrak{V}$ bzw. $\mathfrak{W}$. Definiere die **Summe** $\mathfrak{P} \oplus \mathfrak{Q}$ von $\mathfrak{P}$ und $\mathfrak{Q}$ wie folgt. Setze $\mathfrak{P} \oplus \mathfrak{Q} := \langle P + Q, \leq' \rangle$. $P + Q := P \times \{0\} \cup Q \times \{1\}$. Es sei $\langle x, i \rangle \leq' \langle y, j \rangle$ genau dann, wenn $i = j$ und $x \leq y$. (Also: zwei Elemente sind vergleichbar genau dann, wenn sie aus demselben Summanden stammen und dort vergleichbar sind.) Zeigen Sie, daß die Ordnung der irreduziblen Elemente von $\mathfrak{V} \times \mathfrak{W}$ die Summe der Ordnungen der irreduziblen Elemente von $\mathfrak{P}$ und von $\mathfrak{Q}$ ist, also $\mathfrak{P} \oplus \mathfrak{Q}$. Dh es gilt

$$\mathfrak{Vb}(\mathfrak{V} \times \mathfrak{W}) \cong \mathfrak{Vb}(\mathfrak{V}) \oplus \mathfrak{Vb}(\mathfrak{W})$$

Übung 7. Zeigen Sie, daß ein linearer Verband distributiv ist.

Übung 8. Zeigen Sie: in einem endlichen Verband ist ein Element $\sqcup$–irreduzibel genau dann, wenn es genau einen unteren Nachbarn hat.

Übung 9. Prüfen Sie, ob die folgenden Verbände distributiv sind.



Hinweis. Verwenden Sie den Darstellungssatz. (Bei 5 Elementen würde der Nachweis der Distributivität bei blindem Ausrechnen das Prüfen von 125 Möglichkeiten erfordern!) Bestimmen Sie die irreduziblen Elemente und prüfen Sie, ob die übrigen Elemente eindeutig durch nach unten abgeschlossene Menge dargestellt werden können.

Übung 10. Beweisen Sie Satz 0.19.

Teil 3. Verbände und Boolesche Algebren III. Boolesche Algebren

Ein **Verband mit Null und Eins** ist ein Tupel $\langle V, 0, 1, \sqcap, \sqcup\rangle$, wo $\langle V, \sqcap, \sqcup\rangle$ ein Verband, $0 \in V$ eine Null und $1 \in V$ eine Eins ist. Ein Element $x \in V$ heißt ein **Atom**, falls es ein Nullelement gibt und $y < x$ genau dann gilt, wenn $y = 0$ (also wenn x die Dimension 1 hat). Dual dazu sagt man, $x \in V$ ist ein **Coatom**, falls es eine Eins gibt und $y > x$ nur dann gilt, wenn $y = 1$.

Definition 0.23 *Es sei $\mathfrak{V}$ ein Verband mit Null und Eins und $x \in V$. Ein Element $y \in V$ heißt* ***Komplement*** *von x, falls $x \sqcap y = 0$ und $x \sqcup y = 1$.*

Ist y Komplement von x, so ist x auch Komplement von y. Komplemente muß es nicht geben, auch nicht, wenn der Verband distributiv ist. Zum Beispiel hat in einem linearen Verband mit mehr als zwei Elementen kein Element ein Komplement. Solche Verbände sind aber distributiv. Trotzdem gilt folgender Satz.

Hilfssatz 0.24 *Es sei $\mathfrak{V}$ ein distributiver Verband mit Null und Eins. Sind y_1 und y_2 Komplemente von x, so ist $y_1 = y_2$.*

Beweis. Es ist $y_1 = y_1 \sqcap 1 = y_1 \sqcap (x \sqcup y_2) = (y_1 \sqcap x) \sqcup (y_1 \sqcap y_2) = 0 \sqcup (y_1 \sqcap y_2) = y_1 \sqcap y_2$. Also $y_1 \leq y_2$. Ebenso zeigt man $y_2 \leq y_1$. Q. E. D.

Definition 0.25 *Es sei B eine nichtleere Menge. $\mathfrak{B} = \langle B, 0, 1, -, \cap, \cup \rangle$ ist eine* ***Boolesche Algebra****, falls $0, 1 \in B$, $-$ eine einstellige und $\cap$ und $\cup$ zweistellige Funktionen sind derart, daß $\langle B, 0, 1, \cap, \cup \rangle$ ein distributiver Verband mit Null und Eins ist, und für jedes $x \in B$ $-x$ ein Komplement von x ist. Sei $\mathfrak{C} = \langle C, 0', 1', -', \cap', \cup' \rangle$ eine Boolesche Algebra und $h : B \to C$. h heißt* ***Homomorphismus****, in Zeichen $h : \mathfrak{B} \to \mathfrak{C}$, falls $h(0) = 0'$, $h(1) = 1'$, $h(-x) = -'h(x)$, $h(x \cap y) = h(x) \cap' h(y)$ und $h(x \cup y) = h(x) \cup' h(y)$ ist für alle $x, y \in B$.*

Wir ziehen ein paar Folgerungen aus dieser Definition.

Proposition 0.26 *In einer Booleschen Algebra gelten folgende Gesetze.*

$$\begin{array}{lcl} x \cup -x & = & 1 \\ x \cap -x & = & 0 \\ - - x & = & x \\ -(x \cup y) & = & (-x) \cap (-y) \\ -(x \cap y) & = & (-x) \cup (-y) \end{array}$$

Die letzten beiden Gesetze heißen die ***de Morganschen Gesetze****.*

Beweis. Die ersten beiden Gesetze folgen unmittelbar aus den Definitionen. Ferner ist x das Komplement von $-x$, und da Komplemente ja nunmehr eindeutig sind, ist $- - x = x$. Für das vierte Gesetz muß man zeigen, daß $(x \cup y) \cap ((-x) \cap (-y)) = 0$ und $(x \cup y) \cup ((-x) \cap (-y)) = 1$. Die erste Gleichung ist unmittelbar klar: $(x \cup y) \cap ((-x) \cap (-y)) = (x \cap (-x) \cap (-y)) \cup (y \cap (-x) \cap (-y)) = 0 \cup 0 = 0$. Für die zweite beachte, daß $(x \cup y) \cup ((-x) \cap ((-y)) = (x \cup y \cup (-x)) \cap (x \cup y \cup (-y)) = 1 \cap 1 = 1$. Das fünfte Gesetz ist dual, und wird dual bewiesen. Q. E. D.

Aus dem Darstellungssatz für endliche distributive Verbände folgt nun ein recht schöner Darstellungssatz für Boolesche Algebren. Da Boolesche Algebren distributive Verbände sind (wenn man die Null, die Eins und die Komplementfunktion vergißt), so lassen sich die Elemente von endlichen Booleschen Algebren als Mengen auffassen, und $\cup$ ist die Vereinigung und $\cap$ der Durchschnitt (was wir durch die Notation bereits vorweggenommen haben). Da es immer eine Null und eine Eins gibt müssen wir uns nur noch fragen, für welche distributiven Verbände zu jedem Element ein Komplement existiert. Denn es gilt:

Hilfssatz 0.27 *Es sei $\mathfrak{V} = \langle V, 0, 1, \sqcap, \sqcup \rangle$ ein distributiver Verband, in dem jedes Element ein Komplement hat. Es sei $- : V \to V$ die Funktion, die jedem Element sein Komplement zuordnet. Dann ist $\langle V, 0, 1, -, \sqcap, \sqcup \rangle$ eine Boolesche Algebra.*

Der Beweis ist trivial: der Satz folgt schon aus der Definition.

Hilfssatz 0.28 *Es sei $\mathfrak{V}$ ein distributiver Verband und y ein Komplement von x. Dann ist $\zeta(y)$ das relative Komplement von $\zeta(x)$ in $\mathrm{Irr}(\mathfrak{V})$; das heißt, $\zeta(y) = Irr(\mathfrak{V}) - \zeta(x)$.*

Beweis. Es gilt $\emptyset = \zeta(0) = \zeta(x \sqcap y) = \zeta(x) \cap \zeta(y)$ sowie $Irr(\mathfrak{V}) = \zeta(1) = \zeta(x \sqcup y) = \zeta(x) \cup \zeta(y)$. Q. E. D.

Wir schreiben $-\zeta(x)$ anstelle von $Irr(\mathfrak{V}) - \zeta(x)$.

Hilfssatz 0.29 *Es sei $\mathfrak{V}$ ein endlicher distributiver Verband. Genau dann hat jedes Element ein Komplement, wenn jedes $\sqcup$–irreduzible Element ein Atom ist.*

Beweis. Zunächst einmal ist jedes Atom irreduzibel. Es sei nun jedes irreduzible Element ein Atom. Dann ist jede Teilmenge von $Irr(\mathfrak{V})$ nach unten abgeschlossen. Betrachte die Abbildung ζ. Setze

$$-x := \bigsqcup - \zeta(x)$$

Dann ist $x \sqcap -x = 0$, denn $\zeta(x \sqcap -x) = \zeta(x) \cap \zeta(-x) = \emptyset = \zeta(0)$, und $x \sqcup -x = 1$, da ja $\zeta(x \sqcup -x) = \zeta(x) \cup \zeta(-x) = Irr(\mathfrak{V}) = \zeta(1)$. Nun existiere ein irreduzibles Element u, welches kein Atom ist. Dann existiert ein Atom $x < u$. Die Menge $-\zeta(x)$ ist dann nicht nach unten abgeschlossen. Also hat x kein Komplement. Q. E. D.

Definition 0.30 *Es sei X eine Menge. Die* ***Potenzmengenalgebra*** *über X ist die Boolesche Algebra $\langle \wp(X), 0, 1, -, \cap, \cup \rangle$, bei der $0 = \emptyset$, $1 = X$, $-A := X - A$ sowie $\cap$ und $\cup$ der Mengenschnitt bzw. die Vereinigung sind.*

Satz 0.31 (Darstellungssatz für endliche Boolesche Algebren) *Es sei $\mathfrak{B}$ eine endliche Boolesche Algebra und X die Menge der Atome von $\mathfrak{B}$. Dann ist $\mathfrak{B}$ isomorph zu der Potenzmengenalgebra über X.*

Betrachte nun die Menge $\{0, 1\}$. Setze $\leq := \{\langle 0, 0\rangle, \langle 0, 1\rangle, \langle 1, 1\rangle\}$. Dies ist eine partielle Ordnung. Damit ist

	$-$
0	1
1	0

$\cap$	0	1
0	0	0
1	0	1

$\cup$	0	1
0	0	1
1	1	1

Wir bezeichnen mit **2** die Algebra $\langle \{0, 1\}, 0, 1, -, \cap, \cup \rangle$. Diese Algebra spielt eine wichtige Rolle im Aufbau von Booleschen Algebren.

Hilfssatz 0.32 *Es sei 2^n die Menge aller Folgen der Länge n von Elementen aus $\{0, 1\}$. Sei $\vec{x} \leq \vec{y}$ genau dann, wenn $x_i \leq y_i$ für alle $i \leq n$. Dann ist*

$$\begin{array}{lcl} \vec{x} \cap \vec{y} & = & \langle x_i \cap y_i : 1 \leq i \leq n \rangle \\ \vec{x} \cup \vec{y} & = & \langle x_i \cup y_i : 1 \leq i \leq n \rangle \\ -\vec{x} & = & \langle -x_i : 1 \leq i \leq n \rangle \end{array}$$

Diese Algebra ist das n–fache Produkt von ***2*** *mit sich selbst.*

Satz 0.33 *Es sei $\mathfrak{B}$ eine endliche Boolesche Algebra. Dann ist $\mathfrak{B}$ isomorph zu dem n–fachen Produkt von $\mathbf{2}$, wobei n die Anzahl der Atome von $\mathfrak{B}$ ist.*

Beweis. Es sei X die Menge der Atome von $\mathfrak{B}$. Sei $X = \{x_1, x_2, \ldots, x_n\}$. Sei y ein Element aus B. Sei $f(y) = \langle u_i(y) : 1 \leq i \leq n\rangle$, wobei $u_i(y) = 1$ falls $x_i \leq y$ und 0 sonst. Es ist nicht schwer zu zeigen, daß $y \leq z$ genau dann, wenn $f(y) \leq f(z)$. Dies bedeutet, daß f ein Homomorphismus ist von $\mathfrak{B}$ in die Algebra $\mathbf{2} \times \mathbf{2} \times \ldots \mathbf{2}$. Jeder Folge $\vec{u}$ entspricht das Element $\bigcup\langle x_i : u_i = 1\rangle$, also ist die Abbildung f surjektiv. Sie ist injektiv, da $y = z$ genau dann, wenn für jedes $i \leq n$ gilt $x_i \leq y$ genau dann wenn $x_i \leq z$; also ist dies gleichwertig mit $f(y) = f(z)$. Q. E. D.

Übungen

Übung 11. Es sei 2^n die Menge aller n–langen Folgen aus 0 und 1. Ist $\vec{x}, \vec{y} \in 2^n$, so ist der **Hammingabstand** von $\vec{x}$ und $\vec{y}$, $d_H(\vec{x}, \vec{y})$, die Anzahl aller $i \leq n$ sodaß $x_i \neq y_i$. Zeigen Sie: die Dimension von $\vec{x}$ ist gleich $d_H(\vec{0}, \vec{x})$.

Übung 12. Es sei $\mathfrak{B} = \langle B, 0, 1, -, \cap, \cup\rangle$ eine Boolesche Algebra und $x \in B$. Sei $B_x := \{y : x \geq y\}$. Zeigen Sie, daß $\langle B_x, \leq\rangle$ die Ordnung einer Booleschen Algebra ist. Bestimmen Sie die zugehörigen Operationen. Wir bezeichnen die entstehende Boolesche Algebra mit $\mathfrak{B}_x$.

Übung 13. Zeigen Sie, daß die Abbildung $y \mapsto y \cap x$ ein Homomorphismus ist von $\mathfrak{B}$ auf $\mathfrak{B}_x$.

Übung 14. Es seien $\mathfrak{V}$ und $\mathfrak{W}$ endliche Verbände und $h : \mathfrak{V} \to \mathfrak{W}$ ein Homomorphismus. Zeigen Sie, daß $h^{-1}(x)$ entweder leer ist oder ein Intervall in $\mathfrak{V}$.

Übung 15. Ein **Filter** in einer Booleschen Algebra ist eine Menge $F \subseteq B$ derart, daß (1.) $1 \in F$, (2.) falls $x \in F$ und $x \leq y$ so auch $y \in F$, und (3.) sind $x, y \in F$ so auch $x \cap y \in F$. Zeigen Sie, daß für jeden Homomorphismus $h : \mathfrak{B} \to \mathfrak{C}$ von Booleschen Algebren gilt: $h^{-1}(1)$ ist ein Filter.

Teil 4. Halbgruppen und Monoide

Es sei H eine nichtleere Menge und $\cdot : H \times H \to H$ eine Operation. $\cdot$ heißt **assoziativ**, falls für alle x, y und z aus H gilt

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

Definition 0.34 *Ein Paar $\langle H, \cdot\rangle$, wo H eine nichtleere Menge und $\cdot$ eine zweistellige assoziative Operation auf H ist, heißt eine* ***Halbgruppe****. Ist $1 \in H$ ein Element derart, daß für alle $x \in H$ gilt $1 \cdot x = x \cdot 1 = x$, so heißt 1 eine* ***Eins****, und das Tripel $\langle H, 1, \cdot\rangle$ eine* ***Halbgruppe mit Eins*** *oder* ***Monoid****. $\langle H, \cdot\rangle$ is* ***kommutativ*** *oder* ***abelsch****, falls für je zwei Elemente $x, y \in H$ gilt $x \cdot y = y \cdot x$. Sind $\langle H, \cdot\rangle$ ($\langle H, 1, \cdot\rangle$) und $\langle K, \odot\rangle$ ($\langle K, 1', \odot\rangle$) zwei Halbgruppen (Monoide) und $h : H \to K$, so heißt h* ***Homomorphismus*** *von Halbgruppen (Monoiden), falls für alle $x, y \in H$ gilt $h(x \cdot y) = h(x) \odot h(y)$*

(bei Monoiden zusätzlich $h(1) = 1'$). Wir schreiben $h : \langle H, \cdot\rangle \to \langle K, \odot\rangle$, falls h Homomorphismus ist.

Hier sind Beispiele von Halbgruppen und Monoiden.

Beispiel 1. $\langle \mathbb{N}, 1, \cdot\rangle$ ist ein Monoid. Die Multiplikation ist assoziativ, und $1 \cdot x = x \cdot 1 = 1$.

Beispiel 2. $\langle \mathbb{N}, 0, +\rangle$ ist ein Monoid. Man beachte, daß 0 hier technisch gesehen die Rolle der *Eins* in der Halbgruppe spielt. Dies mag verwirrend erscheinen, aber man gewöhnt sich schnell daran. Es ist $\langle \mathbb{N}, +\rangle$ eine Halbgruppe, ebenso $\langle \mathbb{N} - \{0\}, +\rangle$. Allerdings besitzt die letzte Halbgruppe keine Eins.

Beispiel 3. Betrachte eine nichtleere Menge A. Es sei A^* die Menge aller endlichen Folgen über A, die wir mit Vektorpfeil bezeichnen. Die Länge von $\vec{x}$ bezeichnen wir mit $lg(\vec{x})$. Sind $\vec{x}, \vec{y} \in A^*$, so sei $\vec{x} \cdot \vec{y}$ das Ergebnis der Anfügung von $\vec{y}$ an $\vec{x}$. Diese Operation nennt man **Konkatenation**. Das Paar $\langle A^*, \cdot\rangle$ ist eine Halbgruppe. Wir bezeichnen die leere Folge mit ε. Diese ist eine Eins, wie man leicht nachprüft. Also ist $\langle A^*, \varepsilon, \cdot\rangle$ ein Monoid.

Beispiel 4. Sei k eine natürliche Zahl, A eine nichtleere Menge. Es sei $L(A, k)$ die Menge der Folgen der Länge $\leq k$ über A. Es bezeichne $prf_k(\vec{x})$ das Anfangsstück von $\vec{x}$ der Länge k, falls $\vec{x}$ mindestens die Länge k hat, und $\vec{x}$ sonst. Nun definiere die Operation $^\smile$ durch $\vec{x}^\smile\vec{y} := prf_k(\vec{x} \cdot \vec{y})$. Wir wählen $A = \{a, b\}$ und $k = 2$.

$^\smile$	ε	a	b	aa	ab	ba	bb
ε	ε	a	b	aa	ab	ba	bb
a	a	aa	ab	aa	aa	ab	ab
b	b	ba	bb	ba	ba	bb	bb
aa	aa	aa	aa	aa	aa	aa	aa
ab	ab	ab	ab	ab	ab	ab	ab
ba	ba	ba	ba	ba	ba	ba	ba
bb	bb	bb	bb	bb	bb	bb	bb

Die Halbgruppen bzw. Monoide von Beispiel 1 und 2 sind abelsch, die aus 3 und 4 sind es nicht, wie man leicht nachrechnet. Ein Homomorphismus $h : \mathfrak{G} \to \mathfrak{H}$ heißt **Endomorphismus**, falls $\mathfrak{G} = \mathfrak{H}$, **Isomorphismus**, falls h bijektiv ist, und **Automorphismus**, falls h Isomorphimus und Endomorphismus ist.

Die Multiplikation von natürlichen Zahlen ist assoziativ. Man macht von dieser Tatsache Gebrauch, wenn man bei Produkten auf die Klammern verzichtet, indem man zB schreibt $7 \cdot 43 \cdot 2 \cdot 8$. Streng genommen bedeutet Assoziativität aber lediglich, daß man bei drei Multiplikanden auf die Klammern verzichten kann. Es läßt sich aber zeigen, daß daraus bereits folgt, daß ein Produkt aus beliebig vielen Zahlen stets das gleiche Ergebnis liefert, egal wie es geklammert wird. Wir zeigen dies hier allgemein für Halbgruppen. Ist $\langle H, \cdot\rangle$ eine Halbgruppe, so bilden wir wie folgt Terme über H. Ein Element $x \in H$ ist ein Term; sind s, t Terme, so auch $(s \cdot t)$. Zu einem Term assoziieren wir eine Zeichenkette $\kappa(t) \in H^*$ wie folgt. Für $x \in H$ ist $\kappa(x) = x$; ansonsten ist $\kappa((s \cdot t)) = \kappa(s) \cdot \kappa(t)$. Mit anderen Worten, wir vergessen die Klammern. Terme kann man 'ausrechnen'. Auf diese Weise bestimmt jeder Term ein Element aus H, das wir den

Wert des Terms nennen. Der Wert von $x \in H$ ist schlicht x; der Wert von $(s \cdot t)$ ist das Prodult $u \cdot v$, wo u der Wert von s und v der Wert von t ist. ZB ist der Wert von $((2 \cdot 4) \cdot 7) = (8 \cdot 7) = 56$.

Hilfssatz 0.35 *Es sei $\langle H, \cdot \rangle$ eine Halbgruppe. Es seien s und t Terme über H. Falls $\kappa(s) = \kappa(t)$, so haben s und t denselben Wert.*

Beweis. Wir zeigen: mit Hilfe das Assoziativgesetzes läßt sich jeder Term nach links klammern. Dies geschieht natürlich unter Beibehaltung des Werts; denn die Operation ist ja assoziativ auf H. Dabei heißt t **nach links geklammert**, falls $t = h \in H$ oder $t = (s \cdot h)$ für ein $h \in H$. Analog definiert man **nach rechts geklammert**. Die Behauptung wird induktiv über die Länge der Zeichenkette gezeigt. Für Terme mit Zeichenketten der Länge ≤ 2 ist nichts zu zeigen. Sei $s = (t \cdot u)$ ein Term und gelte die Behauptung für alle Terme kleinerer Länge als s. Ist $u = h \in H$, so ist der Term schon nach links geklammert. Sei dies also nicht der Fall. Dann läßt sich t nach links klammern zu einem Term t' und u läßt sich nach rechts klammern zu einem Term $h \cdot u'$. Es ist also s umformbar in folgenden Term

$$(t' \cdot (h \cdot u'))$$

Einmalige Anwendung des Assoziativgesetzes erbringt

$$((t' \cdot h) \cdot u') \ ,$$

also wieder ein linksgeklammerter Term gefolgt von einem rechtsgeklammerten Term. Ist u' noch nicht von der Form $h \in H$, so wiederholt man diese Operation. Auf diese Weise erhält man schließlich einen linksgeklammerten Term. Analog kann man einen rechtsgeklammerten Term bekommen. Q. E. D.

Definition 0.36 *Es sei $\mathfrak{M} = \langle M, 1, \cdot \rangle$ ein Monoid und $X \subseteq M$. Ist $1 \in X$ und X abgeschlossen unter $\cdot$ (das heißt $x \cdot y \in X$ für alle $x, y \in X$) so heißt $\langle X, 1, \cdot_X \rangle$ ein* ***Untermonoid*** *von $\mathfrak{M}$. Hierbei ist $\cdot_X$ die Einschränkung von $\cdot$ auf X, welche normalerweise auch mit $\cdot$ bezeichnet wird. X* ***erzeugt*** *$\mathfrak{M}$, falls das kleinste X enthaltende Untermonoid von $\mathfrak{M}$ genau $\mathfrak{M}$ selbst ist.*

Wir nehmen etwa das Monoid $\langle \mathbb{N}, 1, \cdot \rangle$. Die Menge der Zahlen, welche durch eine gegebene Zahl n (etwa 14) teilbar sind, bilden zusammen mit der 1 ein Untermonoid. Denn sind k_1 und k_2 durch 14 teilbar, so auch $k_1 \cdot k_2$, ebenso wenn $k_1 = 1$ oder $k_2 = 1$. Ist $k_1 = k_2 = 1$, so ist das Produkt $= 1$. Ebenso bilden die Worte über A der Länge $\geq n$, n gegeben, zusammen mit ε ein Untermonoid von $\langle A^*, \varepsilon, \odot \rangle$.

Falls X $\mathfrak{M}$ erzeugt, so kann man jedes Element von M als Produkt $x_1 \cdot x_2 \cdot \ldots \cdot x_k$ bekommen, wobei $x_i \in X$, $1 \leq i \leq k$. (Ausnahme ist 1. Dieses Element muß sowieso in jedem Untermonoid enthalten sein.) Diese Tatsache ist leicht zu zeigen. Wir benutzen sie für folgenden Satz.

Hilfssatz 0.37 *Es seien $\mathfrak{M}$ und $\mathfrak{N}$ Monoide und $\mathfrak{M}$ sei von X erzeugt. Sei $v : X \to N$ irgendeine Abbildung. Dann existiert höchstens ein Homomorphismus $h : \mathfrak{M} \to \mathfrak{N}$ mit $h \restriction X = v$.*

Beweis. Sei $\mathfrak{M} = \langle M, 1, \odot \rangle$ und $\mathfrak{N} = \langle N, 1', \odot' \rangle$. Es seien $h, k : \mathfrak{M} \to \mathfrak{N}$ Homomorphismen und $h \restriction X = k \restriction X$. Sei $m \in M$. Ist $m = 1$, so ist $h(1) = k(1) = 1'$. Sei also $m \neq 1$. Dann existiert eine Darstellung $m = x_1 \cdot x_2 \cdot \ldots \cdot x_k$. Dann ist

$$\begin{array}{rclcl} h(m) & = & h(x_1) \odot' h(x_2) \odot' \ldots \odot' h(x_k) & = & \\ & = & k(x_1) \odot' k(x_2) \odot' \ldots \odot' k(x_k) & = & k(m) \end{array}$$

Q. E. D.

Definition 0.38 *Es sei $\mathfrak{M} := \langle M, 1, \cdot \rangle$ ein Monoid, und $X \subseteq M$ eine Teilmenge. Wir sagen, $\mathfrak{M}$ wird als Monoid von X* ***frei erzeugt****, falls für jedes Monoid $\mathfrak{N} = \langle N, 1', \odot \rangle$ und jede Abbildung $v : X \to N$ genau ein Homomorphismus $h : \mathfrak{M} \to \mathfrak{N}$ existiert, für den $h \restriction X = v$. h heißt der v* ***fortsetzende Homomorphismus*** *und wird mit $\overline{v}$ bezeichnet.*

Satz 0.39 *Das Monoid $\mathfrak{A} = \langle A^*, \varepsilon, \cdot \rangle$ wird von A frei erzeugt.*

Beweis. Sei $\mathfrak{N} = \langle N, 1, \odot \rangle$ ein Monoid und $v : A \to N$. Es gibt wegen Hilfssatz 0.37 höchstens einen Homomorphismus, welcher v fortsetzt, denn $\mathfrak{A}$ wird von A erzeugt. Dieser Homomorphismus wird definiert über die Länge der Folge. Sei $\vec{x}$ von der Länge 0, Dann $\vec{x} = \varepsilon$ und so $\overline{v}(\vec{x}) = 1$. Ist $lg(\vec{x}) = 1$, so ist $\vec{x} \in A$ und $\overline{v}(\vec{x}) = v(\vec{x})$. Nun sei $lg(\vec{x}) > 1$. Dann ist $\vec{x} = \vec{y} \cdot c$ für ein $c \in A$. Setze $\overline{v}(\vec{x}) := \vec{v}(\vec{y}) \odot v(c)$. Keine andere Wahl ist möglich. Sei $\overline{v}$ auf diese Weise definiert. Es bleibt zu zeigen, daß $\overline{v}$ ein Homomorphismus ist. Dazu betrachte man $\vec{x} \cdot \vec{y}$. Dies ist von der Form $x_1 x_2 \ldots x_m y_1 y_2 \ldots y_n$. $\overline{v}(\vec{x} \cdot \vec{y})$ ist daher von der Form $v(x_1) \odot v(x_2) \odot \ldots \odot v(x_m) \odot v(y_1) \odot v(y_2) \odot \ldots \odot v(y_n)$. Da $\odot$ assoziativ ist, ist dies nichts anderes als $\overline{v}(\vec{x}) \odot \overline{v}(\vec{y})$. Q. E. D.

Satz 0.40 *Es seien $\mathfrak{M} = \langle M, 1, \cdot \rangle$ und $\mathfrak{N} = \langle N, 1', \odot \rangle$ Monoide und $X \subseteq M$ sowie $Y \subseteq N$ Mengen gleicher Mächtigkeit. Es sei $\mathfrak{M}$ von X und $\mathfrak{N}$ von Y frei erzeugt. Dann ist $\mathfrak{M}$ isomorph zu $\mathfrak{N}$.*

Beweis. Da X und Y gleichmächtig sind, existiert eine bijektive Abbildung $v : X \to Y$. Setze $w := v^{-1}$. w ist auch bijektiv. Ferner ist $v \circ w = 1_Y : Y \to Y : y \mapsto y$ sowie $w \circ v = 1_X : X \to X : x \mapsto x$. Nach Voraussetzung über $\mathfrak{N}$ existiert genau ein Homomorphimus $\overline{v \circ w} : \mathfrak{N} \to \mathfrak{N}$. Einen Homomorphismus können wir angeben, nämlich die Identität auf N. Daher ist $\overline{v \circ w} = 1_N$. Ebenso ist die Identität ein Homomorphismus auf $\mathfrak{M}$ und setzt $w \circ v$ fort. Also $\overline{w \circ v} = 1_M$. Nun betrachten wir die Abbildung $\overline{v} \circ \overline{w}$. Diese ist ein Homomorphismus und $\overline{v} \circ \overline{w} \restriction Y = 1_Y$. Daher ist $\overline{v} \circ \overline{w} = 1_N$. Ebenso zeigt man, daß $\overline{w} \circ \overline{w} = 1_M$ ist. Also existieren bijektive Homomorphismen zwischen $\mathfrak{M}$ und $\mathfrak{N}$, die zueinander invers sind. Daher ist $\mathfrak{M} \cong \mathfrak{N}$. Q. E. D.

Dies zeigt in Verbindung mit Satz 0.39, daß die Monoide bestehend aus den Worten über einem Alphabet bis auf Isomorphie die einzigen frei erzeugten Monoide sind. Ferner kommt es bei dem Alphabet nur auf seine Mächtigkeit an.

Zum Schluß erwähnen wir noch eine Konstruktion, welche uns schon bei den Verbänden begegnet ist.

Definition 0.41 *Es seien* $\mathfrak{M} = \langle M, 1, \cdot \rangle$ *und* $\mathfrak{N} = \langle N, 1', \cdot' \rangle$ *Monoide. Dann ist das* ***Produkt*** *von* $\mathfrak{M}$ *und* $\mathfrak{N}$, $\mathfrak{M} \times \mathfrak{N}$, *definiert durch*

$$\mathfrak{M} \times \mathfrak{N} := \langle M \times N, 1'', \cdot'' \rangle$$

wobei $1'' := \langle 1, 1' \rangle \in M \times N$ *und*

$$\langle x_1, y_1 \rangle \cdot'' \langle x_2, y_2 \rangle := \langle x_1 \cdot x_2, y_1 \cdot' y_2 \rangle$$

Es ist nicht schwer zu zeigen, daß die so definierte Struktur ein Monoid ist. Analog definiert man das Produkt von Halbgruppen.

Definition 0.42 *Eine Halbgruppe hat die* ***eindeutige Kürzungseigenschaft****, falls jede Gleichung* $x \cdot g = h$ *bzw.* $g \cdot y = h$ *eine eindeutig bestimmte Lösung für* x *und* y *hat, für jedes* $g, h \in H$.

Eine Halbgruppe mit eindeutiger Kürzungseigenschaft heißt auch **lateinisches Quadrat**. Es ist zum Beispiel $\langle A^*, \cdot \rangle$ ein lateinisches Quadrat. Die Halbgruppe aus Beispiel 4 ist dagegen kein lateinisches Quadrat. Denn es ist $\mathrm{aa}^{\smile}\mathrm{ab} = \mathrm{aa}^{\smile}\mathrm{bb}$, aber $\mathrm{ab} \neq \mathrm{bb}$.

Definition 0.43 *Es sei* $\langle H, 1, \cdot \rangle$ *ein Monoid.* y *heißt* ***linksinvers*** *zu* x*, falls* $y \cdot x = 1$*, und* ***rechtsinvers*** *zu* x*, falls* $x \cdot y = 1$.

Hilfssatz 0.44 *Es sei* $\mathfrak{H}$ *ein Monoid. Genau dann ist* y *linksinvers zu* x*, wenn* x *rechtsinvers zu* y *ist. Ist* y_1 *linksinvers zu* x_1*,* y_2 *linksinvers zu* x_2*, so ist* $y_2 \cdot y_1$ *linksinvers zu* $x_1 \cdot x_2$.

Satz 0.45 *Genau dann hat ein Monoid die eindeutige Kürzungseigenschaft, wenn es zu jedem Element eindeutig bestimmte linksinverse und eindeutig bestimmte rechtsinverse Elemente gibt.*

Definition 0.46 *Eine Struktur* $\mathfrak{G} = \langle G, 1, ^{-1}, \cdot \rangle$ *heißt* ***Gruppe****, falls* $\langle G, 1, \cdot \rangle$ *ein Monoid ist und* x^{-1} *sowohl linksinvers als auch rechtsinvers ist zu* x.

In einer Gruppe gelten also folgende Gesetze

$$\begin{array}{lcl} x \cdot (y \cdot z) & = & (x \cdot y) \cdot z \\ x \cdot 1 & = & x \\ 1 \cdot x & = & x \\ (x \cdot y)^{-1} & = & y^{-1} \cdot x^{-1} \\ x \cdot x^{-1} & = & 1 \\ x^{-1} \cdot x & = & 1 \end{array}$$

Das vierte Gesetz folgt unmittelbar aus der Tatsache, daß $y^{-1} \cdot x^{-1}$ linksinvers ist zu $x \cdot y$ und daß (links)inverse Elemente eindeutig sind:

Hilfssatz 0.47 *Jede Gruppe hat die eindeutige Kürzungseigenschaft. Insbesondere hat jedes Element genau ein linksinverses Element und genau ein rechtsinverses Element, und diese sind gleich.*

Der Beweis ist als Übung überlassen.

Hilfssatz 0.48 *Es sei $\mathfrak{H}$ ein Halbgruppe. Es besitze $\mathfrak{H}$ eine Eins, und es existiere für jedes x ein Element y mit $x \cdot y = y \cdot x = 1$. Setze dann $x^{-1} := y$. Dann ist $\langle H, 1, ^{-1}, \cdot \rangle$ eine Gruppe.*

Viele Autoren reden von einer Halbgruppe $\langle H, \cdot \rangle$ als einer *Gruppe*, falls sie die in dem Hilfssatz 0.48 aufgeführten Bedingungen erfüllt. Denn dann kann man ja solche Operationen hinzufügen, daß aus der Halbgruppe eine Gruppe in obigem Sinne wird. Dennoch sind die Begriffe technisch verschieden. Deshalb ist es besser, eine Halbgruppe *gruppenartig* zu nennen, wenn sie eine Eins besitzt und zu jedem Element x ein y existiert, das sowohl links– wie rechtsinvers ist zu x.

Übungen

Übung 16. Zeigen Sie, daß $\langle \{1, 2, 3\}, \cdot \rangle$ eine Halbgruppe ist mit

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

Gibt es eine Eins?

Übung 17. Es sei auf einer Menge G die folgende zweistellige Operation erklärt: $x \diamond y := x$. Ist $\langle G, \diamond \rangle$ eine Halbgruppe? Ferner: sei $\langle G, \odot \rangle$ eine Halbgruppe und $1 \notin G$. Definiere $\circ$ durch $x \circ y := x \odot y$, falls $x, y \in G$, $1 \circ x := x$ und $x \circ 1 = x$. Ist $\langle G \cup \{1\}, 1, \circ \rangle$ ein Monoid?

Übung 18. Es sei $A = \{a, b\}$ und $B \supseteq A$ ein endliches Alphabet. Zeigen Sie: das von B frei erzeugte Monoid $\mathfrak{F}_M(B)$ läßt sich in das von A frei erzeugte Monoid $\mathfrak{F}_M(A)$ einbetten. Dies bedeutet nichts weiter, als daß es einen injektiven Homorphismus von $\mathfrak{F}_M(B) \to \mathfrak{F}_M(A)$ gibt. *Hinweis.* Den Homomorphismus muß man nur auf den Erzeugern, also den Elementen von B, festlegen. Man braucht also nur eine Zuordnung $\varphi : B \to A^*$ derart, daß zu je zwei Worten über B das φ–Bild jeweils verschieden ist. Die Motivation hinter dieser Aufgabe ist die folgende. Verschiedene Sprachen benutzen verschiedene Alphabete, das Chinesische benutzt ein Alphabet aus mehreren Tausend Zeichen, europäische Sprachen Alphabete in der Größenordnung von 50 bis 100 Zeichen. Das Morsealphabet benutzt 3 (!) Zeichen, Computer nur zwei. Trotzdem kann man alles, was in einem Alphabet notiert werden kann, auch in einem beliebigen anderen Alphabet notieren.

Übung 19. Es sei k eine natürliche Zahl. Definiere $m \oplus_k n := k$ falls $m + n \geq k$, und $m \oplus_k n := m + n$ sonst. Zeige: $\langle \{0, 1, 2, \ldots, k\}, 0, \oplus_k \rangle$ ist eine Halbgruppe.

Übung 20. Zeigen Sie Hilfssatz 0.47.

Teil 5. Kombinatorik I. Binomialkoeffizienten.

Es sei M eine beliebige Menge. Dann bezeichnen wir mit $\sharp M$ die Anzahl der Elemente von M, genannt die **Mächtigkeit** von M. Im Folgenden setzen wir stets voraus, daß Mengen endlich sind. Dann ist die Mächtigkeit eine natürliche Zahl. 0 ist eine natürliche Zahl, und es gibt genau eine Menge M mit $\sharp M = 0$, nämlich die leere Menge, bezeichnet mit $\emptyset$. Wir betrachten nun ein paar Konstruktionen aus der Mengenlehre und schauen nach, wie sich die Anzahlen der konstruierten Mengen bestimmen. Zunächst ein Satz, der sich unmittelbar aus den Definitionen ergibt.

Hilfssatz 0.49 *Es seien M und N endliche Mengen. Genau dann ist $\sharp M = \sharp N$, wenn eine bijektive Abbildung $f : M \to N$ existiert.*

Satz 0.50 *Es seien M und N endlich Mengen. Dann ist*

$$\sharp(M \cup N) = \sharp M + \sharp N - \sharp(M \cap N)$$

Ist insbesondere M disjunkt zu N, so ist

$$\sharp(M \cup N) = \sharp M + \sharp N$$

Satz 0.51 *Es seien M_i, $1 \leq i \leq n$, Mengen. Dann ist*

$$\sharp(M_1 \times M_2 \times \ldots \times M_n) = \prod_{i=1}^{n} \sharp M_i$$

Satz 0.52 *Es seien M und N endliche Mengen, $m := \sharp M$, $n := \sharp N$. Es bezeichne N^M die Menge aller Funktionen von M nach N. Dann ist*

$$\sharp N^M = n^m$$

Beweis. Es sei $M = \{x_1, x_2, \ldots, x_m\}$. Einer Funktion $f : M \to N$ ordnen wir die Folge $\Phi(f) := \langle f(x_1), f(x_2), \ldots, f(x_m)\rangle$ zu. Diese Zuordnung ist bijektiv. $\Phi : N^M \to N \times N \times \ldots \times N$ (m–mal). Also ist nach Satz 0.51 $\sharp N^M = \prod_{i=1}^{m} n = n^m$. Q. E. D.

Wir wollen nun als erstes ein nicht so einfaches Problem betrachten, welches in vielen verschiedenen Gewändern auftritt. Einige äquivalente Formulierungen wollen wir auch angeben, bevor wir daran gehen, diese Zahlen durch explizite Formeln zu bestimmen. Es sei M eine endliche Menge und k eine natürliche Zahl. Dann bezeichne $\binom{M}{k}$ die Menge der k–elementigen Teilmengen von M. Wir interessieren uns für die Anzahl der Elemente der Menge $\binom{M}{k}$, also der Anzahl der k–elementigen Teilmengen von M. Falls $\sharp M = n$, so sei diese Anzahl mit $\binom{n}{k}$ bezeichnet. Es ist klar, daß diese Anzahl nur von $\sharp M$ abhängt. Bevor wir also zur Bestimmung von $\binom{n}{k}$ übergehen, wollen wir uns Anzahlprobleme ansehen, welche auch zu den Zahlen $\binom{n}{k}$ führen.

Problem 1. Es sei $\mathfrak{B}$ eine Boolesche Algebra. Sei $d(\mathfrak{B}, k)$ die Anzahl der Elemente der Dimension k in $\mathfrak{B}$. Nach dem Darstellungssatz für endliche Boolesche Algebren können wir annehmen, $\mathfrak{B}$ sei die Potenzmengenalgebra einer

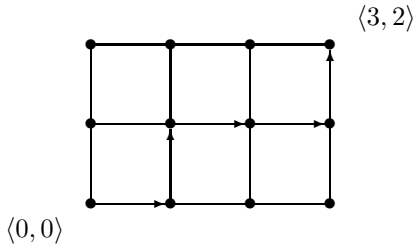
Menge X. Die Elemente von $\mathfrak{B}$ sind die Teilmengen X; die irreduziblen Elemente sind die Atome, dh die Mengen der Form $\{x\}$, $x \in X$. Die Dimension von $Y \subseteq X$ ist genau die Anzahl der Atome unterhalb von Y, und dies ist nichs anderes als die Anzahl der Elemente von Y. Die Elemente von $\mathfrak{B}$ der Dimension k entsprechen somit eineindeutig den k–elementigen Teilmengen von X. Sei nun $n := \sharp X$. Dann ist also $d(\mathfrak{B}, k) = \binom{n}{k}$.

Problem 2. Es sei $m(n,k)$ die Anzahl aller Folgen der Länge n über $\{a,b\}$, welche a genau k mal enthalten. Wir betrachten die Abbildung X, welche der Folge $F = x_1 x_2 \dots x_n$ die Menge $X(F) := \{i : x_i = a\}$ zuordnet. Es ist $X(F) \subseteq \{1, 2, \dots, n\}$. X ist bijektiv. Genau dann kommt a in F k–mal vor, wenn $\sharp X(F) = k$. Also haben wir eine Bijektion zwischen den Folgen, welche a k–mal enthalten und den Teilmengen von $\{1, 2, \dots, n\}$ der Mächtigkeit k. Also ist $m(n,k) = \binom{n}{k}$.

Problem 3. Der Term $(x+y)^n$ kann in eine Summe von Termen der Form $a(n,k)x^k y^{n-k}$ zerlegt werden, wobei $0 \le k \le n$. Allgemein bekannt ist der Fall $n = 2$: $(x+y)^2 = x^2 + 2xy + y^2$. Also $a(2,0) = 1$, $a(2,1) = 2$ und $a(2,2) = 1$. Wir fragen nach den Zahlen $a(n,k)$. Dazu überlegen wir wie folgt. Offensichtlich kann man $(x+y)^n$ stur ausmultiplizieren; dann entsteht eine Summe von Termen der Form $u_1 u_2 \dots u_n$, wobei $u_i = x$ oder $u_i = y$. Wir nennen dies einen **Elementarsummanden** von $(x+y)^n$. Jeder Elementarsummand kommt in dieser Summe genau einmal dran. Da beim Multiplieren die Reihenfolge unerheblich ist, können wir einen Elementarsummanden umschreiben in $x^k y^{n-k}$ für ein $k \le n$. Dabei ist k gerade die Anzahl aller i für die $u_i = x$. Um also die Zahl $a(n,k)$ zu finden, müssen wir letztlich nur wissen, wie viele Folgen $U = u_1 u_2 \dots u_n$ es gibt, in denen x genau k mal auftritt. Also ist nach dem vorigen Problem $a(n,k) = \binom{n}{k}$.

Problem 4. Es sei ein Gitter von Punkten der Ebene gegeben. Es bestehe aus den Punkten (i,j), wo $0 \le i \le m$ und $0 \le j \le n$. Ein **Weg der Länge** k in dem Gitter ist eine Folge von Punkten $P_0, P_1, P_2, \dots, P_k$, wo P_{i+1} jeweils Nachbar von P_i ist. Der Abstand zwischen zwei Punkten P und Q des Gitters, $d(P,Q)$ist das kleinste k derart, daß ein Weg von P nach Q der Länge k existiert. Ist $P = (p_1, p_2)$ und $Q = (q_1, q_2)$, so ist $d(P,Q) = |p_1 - q_2| + |p_2 - q_2|$. Es interessiert uns die Anzahl der kürzesten Wege zwischen P und Q. Wir nennen sie $w(m,n)$. Das folgende Bild zeigt eine kürzesten Weg von $\langle 0,0 \rangle$ nach $\langle 3,2 \rangle$, nämlich

$$\langle 0,0 \rangle, \langle 1,0 \rangle, \langle 1,1 \rangle, \langle 2,1 \rangle, \langle 3,1 \rangle, \langle 3,2 \rangle$$



(Eine Anwendung: der Stadtplan vieler amerikanischer Städte entspricht einem solchen Gitter. Um von einer beliebigen Kreuzung zu einer anderen zu gelanden, kann man nur entlang des Gitters laufen. Der Abstand wie oben definiert ist gerade die sogennante **Taximetrik**, sofern das Gitter aus quadratischen Zellen besteht. Denn dieser Abstand bestimmt ziemlich genau die Rechnung, die man fürs Taxi bezahlen muß...) Man kann sich überlegen, daß es reicht, wenn man $P = (0,0)$ wählt, und $Q = (m,n)$. Der Abstand ist gerade $m+n$. Ein kürzester Weg $W = (P, P_1, P_2, \ldots, P_{n+m})$ geht dann immer nach rechts oder oben, niemals nach links oder unten. Das bedeutet, daß wenn $P_i = (p_i, q_i)$ ist, so ist $P_{i+1} = (p_i + 1, q_i)$ oder $P_{i+1} = (p_i, q_i + 1)$. Einem solchen Weg ordnen wir eine Folge $O(W) = \langle \eta_i : 1 \leq i \leq m+n \rangle$ der Länge $m+n$ zu, wo $\eta_i = o$ falls $P_i = (p_{i-1} + 1, q_{i-1})$ und $\eta_i = r$, falls $P_i = (p_{i-1}, q_{i-1} + 1)$. Die Vorschrift $W \mapsto O(W)$ definiert eine Bijektion zwischen den kürzesten Wegen von $(0,0)$ nach (m,n) und den $n+m$–langen Folgen über $\{o, r\}$, welche genau n mal o enthalten. Also ist $w(m,n) = \binom{m+n}{n}$.

Gehen wir nun zu der Bestimmung von $\binom{n}{k}$ über. Dazu zunächst noch ein neues Zählprinzip. Es sei M eine Menge und $\Pi \subseteq \wp(M) - \{\emptyset\}$ eine Menge von Teilmengen von M. Π heißt **Partition** von M, falls jedes Element von M in genau einer Menge von Π liegt. Ist $\Pi = \{P_1, P_2, \ldots, P_k\}$, so ist natürlich $\sharp M = \sum_{i=1}^{k} \sharp P_i$. Der besondere Fall, wo alle P_i die gleiche Mächtigkeit haben, ist besonders hervorhebenswert.

Hilfssatz 0.53 *Es sei M eine Menge und $\Pi \subseteq \wp(M)$ eine Partition von M, bei der alle Mengen die gleiche Mächtigkeit p haben. Dann ist $\sharp M = p \cdot \sharp \Pi$.*

Wir wählen nun als M die Menge aller Folgen der Länge k von Elementen aus N, wobei kein Element wiederholt werden darf. Es habe N die Mächtigkeit n. Dann gibt es genau

$$n^{\underline{k}} := n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$$

Elemente in M. Zu jeder Folge $F = (x_1, x_2, \ldots, x_k)$ sei $\mu(F) := \{x_1, x_2, \ldots, x_k\}$. Da F kein Element wiederholt, ist $\sharp\mu(F) = k$. Betrachte nun zu jeder k–elementigen Teilmenge X von N die Menge $\Phi(X) := \{F : \mu(F) = X\}$. Dann ist das System

$$\Pi := \{\Phi(X) : X \subseteq N, \sharp X = k\}$$

eine Partition von M. Ferner hat jedes $\Phi(X)$ die gleiche Anzahl Elemente, nämlich $k^{\underline{k}}$. Für letzteren Ausdruck überlegt man sich, daß er gleich $k!$ ist. Nach dem Hilfssatz 0.53 ergibt sich nun

Satz 0.54

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{k!(n-k)!}$$

Übungen

Übung 21. Ein Lottoziehung ist eine Ziehung von 6 Zahlen aus 49. Wie viele verschiedene Ziehungen gibt es? Angenommen, man darf 7 Zahlen tippen. Wie

hoch ist die Wahrscheinlichkeit, 6 bzw. 5 bzw. 4 richtige Zahlen getippt zu haben? (Hier ist Wahrscheinlichkeit die Anzahl der gewünschten Ergebnisse geteilt durch die Anzahl aller möglichen Ergebnisse.)

Übung 22. In einem Verband bezeichne $d(x)$ die Dimension des Elementes x. Man beweise folgende Dimensionsformel für distributive Verbände.

$$d(x \sqcap y) + d(x \sqcup y) = d(x) + d(y)$$

Hinweis. Bedienen Sie sich der Tatsache, daß $d(x) = \sharp\zeta(x)$.

Übung 23. Wir betrachten eine Abstimmung, an der genau n Personen beteiligt sind; es wird ferner nur über eine Sache abgestimmt, und man darf nur mit 'ja' oder 'nein' stimmen. (Es gibt also keine Enthaltungen.) Ergebnisse der Abstimmung sind: 'ja', 'nein', 'unentschieden'. Wie stark ist das Gewicht einer einzelnen Stimme? Intuitiv würde man sagen, das Gewicht sei $1/n$. Ein amerikanischer Richter namens Banzhaff wollte es genauer wissen. Er definierte das Gewicht einer Stimme als die Anzahl der Situationen, in der diese eine Stimme den Ausschlag gibt geteilt durch die Anzahl aller möglichen Situationen. Man stellt sich dabei vor, daß zunächst alle anderen Personen abstimmen und bekommt ein Ergebnis E. Dann wirft man seine Stimme in den Ring und bekommt das endgültige Ergebnis E'. Wenn $E' \neq E$, so hat die eigene Stimme den Ausschlag gegeben. Man nennt das so definierte Gewicht den **Banzhaff–Index**. Wir notieren ihn $bz(n)$. Wie groß ist $bz(7)$? Was läßt sich in Bezug auf die naive Hypothese sagen? Wenn Sie können, geben Sie eine Formel für $bz(n)$ an. *Hinweis.* Man wird nicht umhin kommen, in der Formel für $bz(n)$ zwischen geraden n und ungeraden n zu unterscheiden. Dies spiegelt sich im Übrigen auch in der Art der Ergebnisse E und E' wider.

Übung 24. An einem Bridgeturnier nehmen $4n$ Personen teil, die an n Tischen spielen. Jeder Spieler benötigt einen Partner, und jedes Paar Spieler benötigt ein weiteres Paar als Gegner. Eine Konfiguration ist eine Einteilung von Spielern in Gruppen bestehend aus zwei Paaren. Wie viele Konfigurationen gibt es?

Übung 25. In einem Haus wohnen Autobesitzer, die zusammen a Autos besitzen, und es gibt genau p Parkplätze. Auf wie viele Weisen können die Autobesitzer ihre Autos auf die Parkplätze stellen? *Anmerkung.* Wir nehmen an, daß die größtmögliche Anzahl Autos auf die Stellplätze geparkt wird. Ist $p \geq a$, so werden alle Autos geparkt. Falls aber $p < a$, so müssen einige Autos halt woanders geparkt werden ...

Teil 6. Kombinatorik II. Permutationen.

Es sei im Folgenden stets $N = \{1, 2, \ldots, n\}$. Eine bijektive Abbildung von N auf sich heißt eine **Permutation**. Permutationen spielen in der gesamten Mathematik eine wichtige Rolle. Sind π und ρ Permutationen, so auch $\pi \circ \rho$, definiert durch $(\pi \circ \rho)(x) := \pi(\rho(x))$. (Man beachte also, daß erst ρ und dann π angewendet wird.) Ferner ist π^{-1} eine Permutation, wobei $\pi^{-1}(x) = y$, für das eindeutig bestimmte y mit $\pi(y) = x$. Schließlich ist die Identitäzsabbildung,

bezeichent mit id_N, eine Permutation auf N. Die Permutationen bilden mit diesen Operationen eine Gruppe, die sogenannte **symmetrische Gruppe**. Dies kann man leicht nachrechnen.

Eine Permutation von N können wir notieren, indem wir für jedes Element einzeln das Bild angeben. Sei etwa π eine Permutation, so schreiben wir

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

Daraus leitet man leicht ab, daß es genau $n!$ Permutationen auf N gibt, wenn N genau n Elemente enthält. Denn jede Permutation ist eindeutig durch die untere Zeile bestimmt. Diese ist eine Folge der Länge n, in der kein Element doppelt auftritt. Davon gibt es genau $n!$ Stück.

Bequemer als die eben gezeigte Darstellung ist die sogenannte Zyklenschreibweise, die wir jetzt entwickeln wollen.

Definition 0.55 *Es sei $\pi : N \to N$ eine Permutation. $M \subseteq N$ heißt* ***unter π abgeschlossen****, falls für alle $x \in M$ gilt $\pi(x) \in M$. Ein* ***Orbit*** *oder eine* ***Bahn*** *von π ist eine kleinste Menge $M \subseteq N$, die unter π abgeschlossen ist. Ist $x \in M$, so heißt M* ***der Orbit*** *oder* ***die Bahn von x unter π****. $\sharp M$ heißt die* ***Länge*** *des Orbits M.*

Ist M ein Orbit der Länge k und $x \in M$, so bekommt man M, indem man alle Elemente der Form $\pi^i(x)$, $0 \leq i < k$, bestimmt.

Satz 0.56 *Es sei $\pi : N \to N$ eine Permutation und M ein Orbit von π der Länge k. Sei schließlich $x \in M$ beliebig gewählt. Dann ist stets $M = \{\pi^i(x) : 0 \leq i < k\}$. Jedes Element ist in einem Orbit von π enthalten.*

Beweis. Sei $x \in M$. Da M unter π abgeschlossen ist, muß $\pi(x) \in M$ sein. Aus dem gleichen Grund ist $\pi^2(x) \in M$, $\pi^3(x) \in M$ und so weiter. Da die Mächtigkeit von M genau k ist, existiert ein $i < k$ mit $\pi^k(x) = \pi^i(x)$. Ist nun $i > 0$, so gilt $\pi^{k-1}(x) = \pi^{i-1}(x)$, da π bijektiv ist. Es gibt also ein $n \leq k$ mit $\pi^n(x) = x$. Also ist $\{\pi^i(x) : 0 \leq i < n\}$ unter π abgeschlossen. Ist $n < k$, so ist M nicht die kleinste unter π abgeschlossene Menge, also kein Orbit. Daher ist $n = k$ und so $M = \{\pi^i(x) : 0 \leq i < k\}$. Für die zweite Behauptung wähle ein $x \in N$ und betrachte die Menge aller $\pi^m(x)$, $m \in \mathbb{N}$. Dies ist unter π abgeschlossen, und die kleinste unter π abgeschlossene Menge. Q. E. D.

Für eine beliebige Permutation π zerfällt also N in eine Partition von Orbits. Um eine Permutation festzulegen, genügt nicht die Angabe der Orbits. Man muß auch wissen, wie π auf den Orbits operiert. Die Einschränkung von π auf einen Orbit nennen wir einen **Zyklus**. Einen Zyklus gibt man an, indem man ein beliebiges Element $x \in M$ herausgreift und eine Liste der Elemente $x, \pi(x), \pi^2(x), \dots$ angibt. Ein Zyklus wird wie folgt notiert:

$$(x, \pi(x), \pi^2(x), \dots, \pi^{k-1}(x)) \ .$$

Dann ist klar, daß x auf $\pi(x)$, $\pi(x)$ auf $\pi^2(x)$ geworfen wird — und so weiter. Ein Beispiel.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 3 & 2 & 8 & 1 & 4 & 6 \end{pmatrix}$$

Diese Permutation besitzt die Orbits $\{1,5,6,8\}$, $\{2,4,7\}$ und $\{3\}$. Wir notieren π also durch

$$(1586)(247)(3)$$

Dies bedeutet nach dem eben Gesagten, daß π 2 auf 4, 4 auf 7 und 7 auf 2 wirft; daß 3 auf 3, 1 auf 5, 5 auf 8, 8 auf 6 und schließlich 6 auf 1 wirft. Diese Darstellung ist eindeutig. Wenn die Menge N feststeht, kann man auf Zyklen der Länge 1 verzichten. Deshalb schreibt man die obenstehende Permutation auch

$$(1586)(247)$$

Wir sagen nun, eine Folge $F = \langle x_1, x_2, \ldots, x_k \rangle$ heißt ein **Zyklus** der **Länge** k, falls $x_i \neq x_j$ für alle $1 \leq i < j \leq k$. Ebenso nennen wir diejenige Abbildung π_F einen **Zyklus** welche definiert ist durch $\pi_F : x_i \mapsto x_{i+1}$, $1 \leq i < k$, $\pi_F : x_k \mapsto x_1$, und $\pi_F : y \mapsto y$, falls y in F nicht vorkommt. Schließlich sei $\mathfrak{F} := \{F_1, F_2, \ldots, F_r\}$ eine Menge von Folgen, von denen je zwei kein Element gemeinsam haben. Diese bestimmen eine Permutation $\pi_{\mathfrak{F}} := \pi_{F_1} \circ \pi_{F_2} \circ \ldots \circ \pi_{F_r}$. (In unserem Beispiel ist also $\mathfrak{F} = \{\langle 1,5,8,6\rangle, \langle 2,4,7\rangle\}$ oder auch $\{\langle 1,5,8,6\rangle, \langle 2,4,7\rangle, \langle 3\rangle\}$. Es gibt allerdings noch mehr Möglichkeiten für $\mathfrak{F}$.) Diese Abbildung kann man auch wie folgt angeben. $\pi_{\mathfrak{F}} : x \mapsto \pi_F(x)$, falls x in F vorkommt, und $\pi_{\mathfrak{F}} : y \mapsto y$ sonst. Das Produkt hängt nicht von der Reihenfolge ab. Dies kann man direkt durch Nachrechnen bestätigen. Dazu nehme man ein beliebiges Element x. Falls x nicht in einem der Zyklen auftritt, so ist $\pi_{\mathfrak{F}}(x) = x$. Ferner ist $\pi_{F_i}(x) = x$ für alle F_i, in denen x nicht auftritt. Sei $x \in F_j$. Dann ist $\pi_{\mathfrak{F}}(x) = \pi_{F_j}(x)$, da auch $\pi_{F_j}(x) \in F_j$ und deswegen $\pi_{F_i}(x) = x$ für alle $i \neq j$. Dieses Argument läßt sich verallgemeinern.

Definition 0.57 *Es sei $f : N \to N$ eine Abbildung. $x \in N$ heißt* ***Fixpunkt*** *von f, falls $f(x) = x$. Wir bezeichnen mit $\mathrm{Fix}(\pi)$ die Menge aller Fixpunkte von π.*

Klar ist, daß x genau dann Fixpunkt einer Permutation ist, wenn $\{x\}$ ein Orbit ist. In der verkürzten Zyklendarstellung läßt man also die Angabe der Fixpunkte fallen.

Hilfssatz 0.58 *Es sei π eine Permutation auf N. Dann ist sowohl $\mathrm{Fix}(\pi)$ als auch $N - \mathrm{Fix}(\pi)$ unter π abgeschlossen. Ferner: ist ρ Permutation auf N, so ist $\mathrm{Fix}(\pi \circ \rho) \supseteq \mathrm{Fix}(\pi) \cap \mathrm{Fix}(\rho)$.*

Der Beweis ist als Übung überlassen.

Satz 0.59 *Es seien π und ρ Permutationen auf N mit $N = \mathrm{Fix}(\pi) \cup \mathrm{Fix}(\rho)$. Dann ist $\pi \circ \rho = \rho \circ \pi$.*

Beweis. Es sei $x \in N$. Ist $x \notin \mathrm{Fix}(\pi)$, so ist $x \in \mathrm{Fix}(\rho)$ und so $\pi \circ \rho(x) = \pi(\rho(x)) = \pi(x)$ und $\rho \circ \pi(x) = \rho(\pi(x)) = \pi(x)$. Denn mit x ist auch $\pi(x) \notin \mathrm{Fix}(\pi)$, also $\pi(x) \in \mathrm{Fix}(\rho)$. Ebenso sieht man, daß für $x \in \mathrm{Fix}(\pi)$ gilt $\pi \circ \rho(x) = \rho \circ \pi(x)$. Q. E. D.

Wir vereinbahren nun im Folgenden, daß wir das Produkt von Zyklen nur durch die Hintereinanderschreibung signalisieren. Ferner unterscheiden wir nicht zwischen dem Zyklus und der induzierten Permutation. Also ist (124) ein Zyklus und auch eine Permutation. Für die Identitätsabbildung schreiben wir (). Das Produkt von disjunkten Zyklen ist also kommutativ. Falls Zyklen nicht disjunkt sind, so kann man nichts sagen, außer daß die Zyklen des Produkts in der Vereinigung der Zyklen der Multiplikanden enthalten sind. Zum Beispiel ist $(123)(245) = (14523)$. Es kann auch zu kurzen Zyklen kommen, zum Beispiel in $(124)(142) = (1)(2)(4) = ()$.

Wir betrachten nun eine Permutation π und die Potenzen π^k. Wir können von vornherein sagen, daß falls M ein Zyklus von π^k ist, so ist M auch ein Zyklus von π. Jeder Zyklus von π ist also eine disjunkte Vereinigung von Zyklen von π^k. Ist nämlich $\pi = \zeta_1\zeta_2\ldots\zeta_r$ eine Zerlegung von π in ein Produkt von Zyklen, so gilt $\pi^k = \zeta_1^k\zeta_2^k\ldots\zeta_r^k$. Als Beispiel nehmen wir $\pi = (1586)(274)$. Dann ist

$$\begin{array}{lclclcl}
\pi & = & (1586)(274) & & \pi^2 & = & (18)(56)(247) \\
\pi^3 & = & (1658) & & \pi^4 & = & (274) \\
\pi^5 & = & (1586)(247) & & \pi^6 & = & (18)(56) \\
\pi^7 & = & (1685)(274) & & \pi^8 & = & (247) \\
\pi^9 & = & (1586) & & \pi^{10} & = & (18)(56)(274) \\
\pi^{11} & = & (1685)(247) & & \pi^{12} & = & ()
\end{array}$$

Was ist nun das kleinste k derart, daß $\pi^k = ()$? Dies nennen wir den **Index** von π. Für einen Zyklus ist die Antwort nicht schwer. Ist Z ein Zyklus der Länge k, so ist k gleichzeitig der Index von der Permutation. Ferner ist $Z^m = ()$ genau dann, wenn m ein Vielfaches des Index von Z ist. Daraus folgt mit Satz 0.59 unmittelbar der

Satz 0.60 *Es sei π eine Permutation. Der Index von π ist das kleinste gemeinsame Vielfache aller Indizes von Zyklen von π.*

Eine **Transposition** ist ein Zyklus der Länge 2.

Satz 0.61 *Jede Permutation kann dargestellt werden als das Produkt von Transpositionen.*

Beweis. Da wir eine Permutation als Produkt von Zyklen darstellen können, genügt es zu zeigen, daß jeder Zyklus das Produkt von gewissen Transpositionen ist. Ohne Beschränkung der Allgemeinheit ist ein Zyklus von der Form $\zeta = (1\ 2\ 3\ldots k)$. Betrachte das Produkt $\pi := (2\ 3)(3\ 4)\ldots(k-1\ k)(k\ 1)$. Man rechnet nach, daß $\pi(1) = 2$, $\pi(2) = 3$ und so weiter, $\pi(k) = 1$. Also $\pi = \zeta$. Q. E. D.

Es sei nun $\theta_1\theta_2\ldots\theta_m = \eta_1\eta_2\ldots\eta_n$ zwei Darstellungen von π als Produkt von Transpositionen. Es gilt nun zwar nicht $m = n$ (wie man leicht sieht, kann man das nicht erwarten), aber wie wir zeigen werden ist $m-n$ stets eine gerade Zahl. Wir nennen deshalb $(-1)^m$ das **Signum** von π. Das Signum eines Zyklusses der Länge k ist also $(-1)^{k-1}$. Da $m-n$ gerade ist, ist nämlich $(-1)^n = (-1)^m$, und so ist diese Zahl unabhängig von der gewählten Darstellung als Produkt. Wir werden dies über einen Umweg beweisen.

Definition 0.62 *Eine $n \times n$–**Permutationsmatrix** ist eine $n \times n$–Matrix mit Einträgen 0 oder 1 derart, daß in jeder Zeile sowie in jeder Spalte genau einmal 1 auftritt.*

Sei e_i derjenige Vektor, welcher genau an der Stelle i eine 1 hat, und sonst 0 ist. Wir schreiben $e_i = (\delta_{ij})_{1 \leq j \leq n}$, wobei $\delta_{ij} = 1$ genau dann, wenn $i = j$, und 0 sonst. (δ_{ij} ist das sogenannte *Kroneckersymbol*, benannt nach LEOPOLD KRONECKER, 1823 – 1891.) Wir können jeder Permutation π genau eine Permutationsmatrix $A(\pi)$ mit $A(\pi) \cdot e_i = e_{\pi(i)}$ für alle $1 \leq i \leq n$. Denn es ist $A(\pi) = (a_{ij})_{1 \leq i,j \leq n}$. Also ist der $k$te Eintrag in $A(\pi) \cdot e_i$ gerade $\sum_{j=1}^{n} a_{kj}\delta_{ji} = a_{ki}$. Dieser muß nun gerade gleich 0 sein, wenn $k \neq \pi(i)$ und 1, falls $k = \pi(i)$. Also haben wir $a_{ij} = 1$ genau dann, wenn $i = \pi(j)$, und 0 sonst. Dies ist eine Permutationsmatrix. Zum Beispiel sei $\pi = (1\ 3\ 4)(2)$. Dann ist

$$A(\pi) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Denn zum Beispiel ist $\pi(1) = 3$. Daher $a_{31} = 1$. Man überzeuge sich, daß $A(\pi)e_1 = e_3$, $A(\pi)e_2 = e_2$, $A(\pi)e_3 = e_4$ sowie $A(\pi)e_4 = e_1$ ist. Sei umgekehrt B eine Permutationsmatrix. Dann ist $B \cdot e_i = e_j$ für ein gewisses j, und man rechnet nach, daß es eine Permutation π geben muß mit $B \cdot e_i = e_{\pi(i)}$. Also $B = A(\pi)$. Ist dies erst einmal etabliert, so betrachte man zwei Permutationen, π und ρ. Es ist $\rho \circ \pi$ eine Permutation, und zu ihr gehört eine Permutationsmatrix, $A(\rho \circ \pi)$. Nun ist $\rho \circ \pi(i) = \rho(\pi(i))$, und so $A(\rho \circ \pi)e_i = A(\rho)(A(\pi)(e_i))$ für alle $1 \leq i \leq n$. Daraus folgt schließlich der

Satz 0.63 *Zu jeder Permutation π existiert eine eindeutig bestimmte Permutationsmatrix $A(\pi)$ mit $A(\pi)e_i = e_{\pi(i)}$ für alle i mit $1 \leq i \leq n$. Ferner gilt $A(\rho \circ \pi) = A(\rho) \circ A(\pi)$.*

Nun definieren wir

$$sgn(\pi) := det(A(\pi))$$

Wir werden zeigen, daß $sgn(\pi)$ unser vorher definiertes Signum ist. Alles andere folgt aus dieser Tatsache.

Hilfssatz 0.64 *Es sei π eine Permutation. Dann gilt*

$$det(A(\pi)) = \pm 1$$

Beweis. Es sei $M = (m_{ij})_{1 \leq i,j \leq n}$ eine $n \times n$–Matrix. Dann bezeichne M^{ij} diejenige $(n-1) \times (n-1)$–Matrix, die aus M durch Streichen der $i$ten Zeile und der $j$ten Spalte hervorgeht. Der Determinantenentwicklungssatz besagt

$$det(M) = \sum_{i=1}^{n} (-1)^{i+1} m_{1i} \cdot det M^{1i}$$

Wir beweisen die Behauptung nun durch Induktion über die Anzahl n der permutierten Elemente. Ist $n = 1$, so ist $A(\pi) = (1)$ und $det(A(\pi)) = 1$. Nun sei die Behauptung für n gezeigt, und sei π eine Permutation über $n+1$ Elemente. Ferner sei i so gewählt, daß $\pi(i) = 1$. Dann ist nach dem Entwicklungssatz

$$det(A(\pi)) = \sum_{i=1}^{n} (-1)^{i+1} a_{1i} \cdot det M^{1i} = (-1)^{j+1} det(A(\pi)^{1j})$$

Hierbei ist $j = \pi^{-1}(1)$. Die Behauptung folgt aus der leicht zu prüfenden Tatsache, daß $A(\pi)^{1j}$ wiederum eine Permutationsmatrix ist. Q. E. D.

Als nächstes benötigen wir den Produktsatz für Determinanten. Dieser besagt, daß $det(A \cdot B) = det(A) \cdot det(B)$. Als letztes benötigen wir noch die Tatsache, daß für eine Transposition τ $det(A(\tau)) = -1$. Dies zeigt man so. Bis auf Umbenennen der Elemente ist $\tau = (12)$. Ist aber π bis auf Umbenennung gleich ρ, so gilt $det(A(\pi)) = det(A(\rho))$. (Denn die Matrix der Umbennung ist eine Permutationsmatrix $A(\sigma)$ und so ist $A(\rho) = A(\sigma)^{-1} A(\pi) A(\sigma)$. Daher ist $det(A(\rho)) = det(A(\pi))$. Wer dies umständlich findet: der Beweis benötigt dies auch nicht wirklich.) Wendet man den Entwicklungssatz an, so bekommt man

$$det(A(\tau)) = det\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = -1 \ .$$

Jetzt folgt: ist π das Produkt von irgendwelchen Transpositionen τ_j, $1 \leq j \leq r$, so ist $sgn(A(\pi)) = (-1)^r$. Daraus folgt unsere Behauptung, daß $sgn(\pi)$ genau das Signum von π ist. Dies bedeutet auch, daß das Signum unabhängig von der gewählten Zerlegung ist, und somit die Anzahl der Transpositionen, aus denen π zusammengesetzt ist, entweder immer gerade ist oder immer ungerade ist.

Übungen.

Übung 26. Zeigen Sie Hilfssatz 0.58.

Übung 27. Es sei Z ein Zyklus der Länge mn, m und n Zahlen. Zeigen Sie, daß Z^m ein Produkt von m Zyklen der Länge n ist.

Übung 28. Es sei π folgende Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 4 & 7 & 6 & 9 & 2 & 3 & 5 & 1 \end{pmatrix}$$

Schreiben Sie π in Zyklendarstellung. Geben Sie die zugehörige Permutationsmatrix an. Welchen Index hat π?

Übung 29. Es seien $\pi := (a_1\ a_2\ \ldots\ a_m)$ und $\rho := (b_1\ b_2\ \ldots\ b_n)$ Zyklen, die genau eine Element gemeinsam haben. Zeigen Sie, daß $\pi \circ \rho$ einen Zyklus der Länge $m + n - 1$ ist. *Hinweis.* Man darf annehmen, daß $a_m = b_1$ ist. Siehe dazu die nächste Aufgabe.

Übung 30. Sei $\pi = (a_1\ a_2\ \ldots\ a_n)$ ein Zyklus. Zeigen Sie, daß

$$\pi = (a_r\ a_{r+1}\ \ldots\ a_n\ a_1\ a_2\ \ldots\ a_{r-1})$$

Teil 7. Kombinatorik III. Verteilungen.

Wir ziehen zunächst noch einige nützliche Folgerungen aus der Definition von $\binom{n}{k}$. Die Anzahl aller $k+1$–elementigen Teilmengen einer Menge mit $n+1$ Elementen kann wie folgt bestimmt werden. Man wähle ein Element $x \in M$. Für $X \subseteq M$ der Mächtigkeit $k+1$ gibt es zwei Fälle. **Fall 1.** $x \in X$. Dann ist X eine $k+1$–elementige Teilmenge von $M - \{x\}$. **Fall 2.** $x \in X$. Dann ist $X - \{x\}$ eine k–elementige Teilmenge von $M - \{x\}$. Dies führt zu folgender Gleichung.

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$$

Aus dieser Vorschrift ergibt sich ein leichtes Verfahren, wie man die Binomialkoeffizienten berechnen kann. Dies ist als das Pascalsche Dreieck bekannt, benannt nach Blaise Pascal (1623 – 1662).

					1						$n=0$
				1		1					$n=1$
			1		2		1				$n=2$
		1		3		3		1			$n=3$
	1		4		6		4		1		$n=4$
1		5		10		10		5		1	$n=5$

Man beginnt mit der ersten Zeile für $n = 0$. Anschließend füllt man das dreieckige Schema aus. Jede Zahl mit Ausnahme der Randzahlen hat zwei obere Nachbarn. Jede Zahl ist die Summe ihrer oberen Nachbarn. Zum Beispiel ist $10 = 4 + 6$, da 10 die oberen Nachbarn 4 und 6 hat.

Ferner haben wir gezeigt, daß $(x+y)^n = \sum_{i=0}^{n} \binom{n}{k} x^k y^{n-k}$. Setzen wir $x = y = 1$, so bekommen wir

$$\sum_{i=0}^{n} \binom{n}{k} = 2^n$$

Dies ist auch deswegen klar, weil $\binom{n}{k}$ die Anzahl der k–elementigen Teilmengen einer n–elementigen Menge ist. Es gibt insgesamt 2^n solcher Teilmengen.

Setzen wir $x = 1$, $y = -1$, dann ergibt sich

$$\sum_{i=0}^{n} (-1)^k \binom{n}{k} = 0$$

Also: die alternierende Summe über die Binomialkoeffizienten ist gleich 0. Etwa ist $1 - 4 + 6 + 4 - 1 = 0$. Ist n ungerade, so folgt dies unmittelbar aus der Tatsache, daß $\binom{n}{k} = \binom{n}{n-k}$ ist sowie mit jedem Term $(-1)^k \binom{n}{k}$ auch der Term $(-1)^{n-k} \binom{n}{n-k} = -(-1)^k \binom{n}{k}$ auftritt.

Im Folgenden wollen wir uns mit Verteilungsproblemen befassen. Einige haben wir schon vorher kennengelernt. Im Wesentlichen ist das Problem so beschrieben. Wir wollen n Bälle auf r Fächer verteilen. Wie viele Möglichkeiten gibt es? Ein analoges Problem ist dieses. Wir haben eine Menge B mit n Elementen und eine Menge F mit r Elementen. Wie viele Funktionen gibt es von B nach F? Dies haben wir schon errechnet. Die Anzahl ist r^n. Wir können nun einerseits Bedingungen an die Funktionen stellen; das heißt, wir bestimmen beispielsweise nur die injektiven, oder nur die surjektiven oder nur die bijektiven Funktionen. Auf der anderen Seite können wir auch von der Identität der Objekte absehen. Das heißt konkret, wir können annehmen, daß die Bälle bzw. die Fächer ununterscheidbar sind. Beide Möglichkeiten werden oft benutzt. Der Unterschied zwischen *unterscheidbar* und *ununterscheidbar* kommt zum Beispiel in dem Unterschied zwischen einer Menge und einer nichtwiederholenden Folge heraus. Die Folge F ordnet jedem Folgenglied einen Platz zu; die zugehörige Menge der Folgenglieder tut dies nicht. Sie sieht von der Reihenfolge ab. Wir veranschaulichen den Unterschied durch ein Beispiel. Es sei $B = \{1, 2, 3, 4\}$ und $F = \{a, b, c\}$. Betrachte folgende Verteilungen:

V_1	V_2
a:()	a:()
b:(1)	b:(234)
c:(234)	c:(1)

V_3	V_4
a:()	a:(3)
b:(3)	b:(124)
c:(124)	c:()

Falls wir sowohl die Bälle unterscheiden wie die Fächer, so sind alle Verteilungen verschieden. Falls wir die Fächer nicht mehr unterscheiden, so sind V_1 und V_2 sowie V_3 und V_4 nicht mehr zu unterscheiden. Am besten sieht man das so: wir entfernen von den Fächern die Namen a, b und c. Dann haben wir nur noch die Information, daß bei V_1 beispielsweise ein Fach keinen Ball, ein anderes den Ball 1 und ein drittes die Bälle 2, 3 und 4 enthält. Anders ausgedrückt: falls wir durch Vertauschen der Namen der Fächer eine Verteilung V in die Verteilung V' überführen können, so sind V und V' in dem Falle gleich, wo wir die Fächer nicht mehr unterscheiden. Man sieht nun ebenso, daß wenn wir die Bälle nicht mehr unterscheiden, nunmehr V_1 und V_3 gleich sind. Falls wir schließlich weder Fächer noch Bälle unterscheiden wollen, so sind alle vier Verteilungen gleich. In der folgenden Definition wollen wir ungeordnete Folgen definieren. Die Definition mag etwas umständlich erscheinen, aber sie ist relativ einleuchtend, wenn man sie von der praktischen Seite her sieht. Eine ungeordnete Folge ist eine Folge, in der es nicht auf den Platz ankommt, den ein Element einnimmt. Dies drücken wir so aus, daß wir eine ungeordnete Folge als die Menge aller geordneten Folgen auffassen, welche durch Umordnung ineinander übergehen.

Definition 0.65 *Es sei X eine Menge, und F und G n–lange Folgen von El-*

ementen aus X. Für $x \in X$ sei $j(x, F)$ die Anzahl der Folgenglieder, welche gleich x sind. Dies heiße der ***Index*** *von x in F. Wir setzen $F \approx G$, falls für alle Elemente x aus X gilt $j(x, F) = j(x, G)$. Die Menge $M(F) := \{G : F \approx F\}$ heißt auch eine* ***Multimenge*** *M mit Elementen aus X oder* ***ungeordnete Folge****. Die* ***Mächtigkeit*** *von M ist definiert als die Länge von F.*

Diese Definition ist nicht besonders handlich. Wir notieren Multimengen so:

$$\{a, b, b, a, c, d, d, a, d\}_m$$

Der Index $_m$ deutet an, daß es sich um eine Multimenge handelt. Mengen sind Multimengen, in denen der Index nur 0 oder 1 ist. Wie auch sonst üblich, ist die oben hingeschriebene Folge nur ein Vertreter. Dieselbe Multimenge ist beschrieben durch

$$\{d, d, d, c, b, b, a, a, a\}_m$$

Nehmen wir also wieder unsere Bälle und Fächer. Seien sowohl Bälle als auch Fächer unterschieden. Dann existieren in der Tat r^n viele Verteilungen. Seien nun die Bälle unterschieden, nicht aber die Fächer. Dann entspricht einer Verteilung schlicht eine Partition der Menge B in genau r Mengen. Ist $r > n$, so existiert keine Partition. Die Anzahl der Partitionen einer n–elementigen Menge in r Mengen bezeichnet man mit $S_{n,r}$. Falls wir nun auch noch die Bälle nicht mehr unterscheiden, so ist die Anzahl der Möglichkeiten gerade die Anzahl der Möglichkeiten, die Zahl n in r von Null verschiedene Summanden zu zerlegen. Diese Zahl nennen wir $P_{n,r}$. Zum Beispiel ist $P_{7,3} = 4$, denn

$$\begin{aligned} 7 &= 1 + 1 + 5 \\ &= 1 + 2 + 4 \\ &= 1 + 3 + 3 \\ &= 2 + 2 + 3 \end{aligned}$$

Über die Zahlen $S_{n,r}$ und $P_{n,r}$ läßt sich keine leichte Berechnungsvorschrift angeben. Es gilt aber folgender Sachverhalt.

Satz 0.66 *Sei $n > 0$. Es ist $P_{n,1} = 1$, $P_{n,2} = \frac{n}{2}$, falls n gerade und $P_{n,2} = \frac{n-1}{2}$, falls n ungerade.*

Beweis. Es ist klar, daß eine beliebige Zahl sich nur auf eine Weise als Summe einer einzigen Zahl darstellen läßt. Nun sei $n = 2k$ eine gerade Zahl. Dann ist für beliebiges i mit $0 < i < n$, $n = i + (n - i)$. Um Doppelzählungen zu vermeiden, überlegen wir uns, daß, falls $i > k$ ist, $n - i < k$ ist. Wir betrachten deswegen nur solche Summen $i_1 + i_2$, in denen $i_1 \leq i_2$ ist. (Dieses Verfahren wendet man ganz allgemein bei der Bestimmung der $P_{n,r}$ an.) Zu jeder Zahl i mit $0 < i \leq k$ gibt es genau eine Zerlegung von n, nämlich $n = i + (n - i)$, und es ist $i \leq n - i$. Für zwei Darstellungen $i + (n - i) = j + (n - j)$ mit $0 < i, j \leq k$ gilt $i = j$. Wir haben also exakt k viele solcher Darstellungen, das heißt genau $\frac{n}{2}$ viele. Falls nun n ungerade ist, also $n = 2k + 1$, muß man beachten, daß wiederum $0 < i \leq k$ muß. Dies ergibt den Wert $\frac{n-1}{2}$. Q. E. D.

Will man $P_{n,r}$ für $r > 2$ exakt ausrechnen, muß man einige Mühe aufwenden. Betrachten wir kurz den Fall $r = 3$. Zwei Darstellungen $n = i_1 + i_2 + i_3$ und $n = j_1 + j_2 + j_3$ sind gleich, falls $\{i_1, i_2, i_3\} = \{j_1, j_2, j_3\}$. Eine Darstellung $n = i_1 + i_2 + i_3$ kann man immer so wählen, daß $i_1 \leq i_2 \leq i_3$. Ist dann $i_1 + i_2 + i_3 = j_1 + j_2 + j_3$ mit $j_1 \leq j_2 \leq j_3$, so gilt $i_1 = j_1$ und $i_2 = j_2$ und $i_3 = j_3$, oder aber es gilt $\{i_1, i_2, i_3\} \neq \{j_1, j_2, j_3\}$ (das heißt, die Darstellungen sind ungleich). Dies bedeutet, daß wir jede Darstellung tatsächlich nur einmal zählen. Nun geht man so vor. Man wählt i_1, und bestimmt die Anzahl aller Darstellungen von $n - i_1$ in Summen $i_2 + i_3$, wo $i_1 \leq i_2 \leq i_3$. Dies bedeutet, wir wollen nur solche Darstellungen von $n - i_1$ betrachten, in denen alle Summanden $\geq i_1$ sind. Man überlege sich, daß dies gerade die Anzahl aller Darstellungen von $n - 3i_1 + 2$ in Summen $k_1 + k_2$, $k_1, k_2 > 0$, ist. Denn ist $n - 3i_1 + 2 = k_1 + k_2$, so ist

$$n - i_1 = (k_1 + i_1 - 1) + (k_2 + i_1 - 1)$$

Mit $k_1 > 0$ ist $k_1 + i_1 - 1 \geq i_1$, und mit $k_1 \leq k_2$ ist $k_1 + i_1 - 1 \leq k_2 + i_1 - 1$. Dies erledigt die Darstellung von $n - i_1$. Nun muß man im Prinzip nur aufsummieren. Man beachte, daß man stets $i_1 \leq \frac{n}{3}$ hat. Größere i_1 muß man nicht betrachten.

Als letztes betrachten wir den Fall, wo zwar die Fächer unterschieden werden, nicht aber die Bälle. Dann ist eine Verteilung einzig bestimmt durch die Anzahl der Bälle, welche in einem gegebenen Fach liegen. Dies entspricht aber genau einer Multimenge über r, in der die Summe der Indizes gerade n ist. Die Summe aller Indizes $j(x, F)$ ist aber gerade die Mächtigkeit der durch F repräsentierten Multimenge. Die Anzahl der Multimengen der Mächtigkeit r über einer Menge B der Mächtigkeit n läßt sich durch einen Trick berechnen. Ohne Beschränkung der Allgemeinheit ist $B = \{1, 2, \ldots, n\}$. Zu jeder Multimenge gibt es genau eine Auflistung der Elemente, die monoton wachsend ist. (Etwa ist $\{1, 1, 2, 2, 3\}_m$ eine solche Auflistung, nicht aber $\{3, 1, 1, 2, 2\}_m$.) Sei $M = \{x_1, x_2, \ldots, x_r\}_m$ eine Multimenge mit $x_i \leq x_{i+1}$. Nun setze $A(M) := \{x_1, x_2 + 1, x_3 + 2, x_4 + 3, \ldots, x_r + r - 1\}$. $A(M)$ ist wohlgemerkt eine Menge, und es ist $x_i + i - 1 < x_{i+1} + i$, nach Wahl der x_i. $A(M)$ ist eine r–elementige Teilmenge von $\{1, 2, \ldots, n + r - 1\}$. Sei $Y \subseteq \{1, 2, \ldots, n + r - 1\}$ eine r–elementige Menge, etwa $Y = \{y_1, y_2, \ldots, y_r\}$ mit $y_i < y_{i+1}$. Dann setze $B(Y) := \{y_1, y_2 - 1, y_3 - 2, \ldots, y_r - r + 1\}$. $B(Y)$ ist der Repräsentant einer Multimenge der Mächtigkeit r über B. Diese Beziehung ist bijektiv. Also ergibt sich folgender Satz.

Satz 0.67 *Die Anzahl der Multimengen der Mächtigkeit k über einer Menge der Mächtigkeit n ist*

$$\frac{(n + k - 1)^{\underline{k}}}{k!}$$

Übungen

In den folgenden Aufgaben werden recht große Zahlen auftreten. Aus diesem Grunde ist es von Vorteil, die Aufgaben stets abstrakt zu lösen und nicht nur auszurechnen (was mit Hilfe des Computers nicht schwer sein dürfte). Man kann schon einiges erreichen, wenn man nur die Formeln bestimmt hat, nach denen

man ausrechnen muß.

Übung 31. Eine Tüte Gummibären enthalte stets genau 50 Gummibären. Gummibären gibt es in genau 3 Farben. Es sei von jeder Farbe mindestens ein Gummibär in einer Tüte enthalten. Wie viele verschiedene Farbmischungsverhältnisse gibt es? Geben Sie zunächst eine Benennung der Zahl in Form einer Formel an (welcher Typ von Zählkoeffizient) und berechnen Sie seinen Wert.

Übung 32. Desgleichen wie in der vorigen Übung, aber ohne die Bedingung, daß eine bestimmte Farbe auftreten muß. *Hinweis.* Vergessen Sie bitte auch diesmal nicht, eine Formel anzugeben, bevor Sie sich an's Ausrechnen machen!

Übung 33. Wie in den vorigen beiden Aufgaben. Nun seien aber die Farben konkret gegeben: rot, gelb und grün. Bestimmen Sie also die Farbmischungsverhältnisse rot:gelb:grün mit und ohne die Bedingung, daß eine Farbe mindestens einmal vertreten sein muß.

Übung 34. Stellen sie alle Verteilungen von drei Kugeln auf drei Fächer dar. Wie viele gibt es wenn man (a) Kugeln und Fächer unterscheidet, (b) nur Fächer unterscheidet, (c) nur Kugeln unterscheidet, (d) weder Kugeln noch Fächer unterscheidet?

Übung 35. Es sei $N = \{1, 2, \ldots, n\}$. Einer Multimenge K über N ordnen wir als *Typ* die Folge $\langle j(1, F), j(2, F), \ldots, j(n, F)\rangle$. Zeige zunächst: jeder Multimenge über N entspricht genau eine Folge natürlicher Zahlen

$$\mathfrak{j} = \langle j(1), j(2), \ldots, j(n)\rangle \ .$$

Gegeben eine solche Folge, bestimmen Sie die Anzahl der geordneten Folgen G, deren ungeordnetes Gegenstück gerade der Multimenge des Typs $\mathfrak{j}$ entspricht. Diese Anzahl bezeichnet man mit

$$\binom{q}{j(1), j(2), \ldots, j(n)}$$

wobei $q = j(1) + j(2) + \ldots + j(n)$. *Hinweis.* Insbesondere ist im Falle $n = 2$ diese Zahl dann $\binom{q}{j(1), j(2)}$, welches (in anderer Notation) der allbekannte Binomialkoeffizient ist.

Teil 8. Graphen I. Grundlegende Definitionen.

Das Material für die folgenden vier Teile wurde überwiegend entnommen aus M. Aigner: *Diskrete Mathematik*, Vieweg Verlag, 1993.

Bevor wir beginnen, wollen wir uns mit dem Rechnen in Restklassen beschäftigen, da dies in Zukunft häufiger auftritt. Es sei n eine beliebige natürliche Zahl, $n > 1$. Dann existiert zu jeder ganzen Zahl k eine Darstellung $k = c \cdot n + r$, wobei $0 \leq r < n$. Diese heißt der **Rest modulo** n von k. Wir schreiben $k \equiv \ell \pmod{n}$ um auszudrücken, daß k und ℓ den gleichen Rest modulo n haben und sagen, *k ist kongruent zu r modulo n.* Die Relation *ist kongruent modulo n* ist eine Äquivalenzrelation, wie man leicht bestätigt. Man überlegt sich ferner, daß

$k \equiv \ell \pmod{n}$ genau dann, wenn es $c, d, r \in \mathbb{Z}$ gibt mit $k = c \cdot n + r$ und $\ell = d \cdot n + r$. Dabei muß r nicht zwischen 0 und $n-1$ liegen! Es gilt folgender Sachverhalt.

Satz 0.68 *Es sei* $k_1 \equiv \ell_1 \pmod{n}$ *und* $k_2 \equiv \ell_2 \pmod{n}$. *Dann ist*

$$k_1 + k_2 \equiv \ell_1 + \ell_2 \pmod{n}, \qquad k_1 \cdot k_2 \equiv \ell_1 \cdot \ell_2 \pmod{n}$$

.

Beweis. Es sei $k_i = c_i \cdot n + r_i$, $\ell_i = d_i \cdot n + r_i$. Dann ist $k_1 + k_2 = (c_1 + c_2) \cdot n + (r_1 + r_2)$ sowie $\ell_1 + \ell_2 = (d_1 + d_2) \cdot n + (r_1 + r_2)$. Also $k_1 + k_2 \equiv r_1 + r_2 \pmod{n}$ und $\ell_1 + \ell_2 \equiv r_1 + r_2 \pmod{n}$. Daher $k_1 + k_2 \equiv \ell_1 + \ell_2 \pmod{n}$. Ebenso sieht man $k_1 \cdot k_2 \equiv \ell_1 \cdot \ell_2 \pmod{n}$, denn es ist $k_1 \cdot k_2 = (c_1 c_2 n + c_1 r_2 + c_2 r_1)n + r_1 r_2$ und ebenso $\ell_1 \cdot \ell_2 = (d_1 d_2 n + d_1 r_2 + d_2 r_1)n + r_1 r_2$. Q. E. D.

Wir können also folgende Addition und Multiplikation auf $\{0, 1, \ldots, n-1\}$ definieren. Es sei $x \oplus_n y$ das eindeutig bestimmte $r \in \{0, 1, \ldots, n-1\}$ mit $x + y \equiv r \pmod{n}$. Ebenso sei $x \odot_n y$ das eindeutig bestimmte $r \in \{0, 1, \ldots, n-1\}$ mit $xy \equiv r \pmod{n}$. Wir schreiben in aller Regel $x + y$ anstelle von $x \oplus_n y$ und $x \cdot y$ anstelle von $x \odot_n y$. Es existiert zu x stets ein Element y mit $x \oplus_n y = 0$. Wir notieren es mit $-x$. Die üblichen Gesetze für Addition, Subtraktion und Multiplikation gelten. Ferner: ist n eine Primzahl, so existiert für jedes $x \neq 0$ ein y mit $x \odot y = 1$. Wir behaupten, daß nämlich $y \neq y'$ bedeutet $x \odot_n y \neq x \odot_n y'$. Andernfalls ist $x \odot_n (y - y') = 0$. Nun ist n eine Primzahl; n teilt das Produkt $x(y - y')$. Da n die Zahl x nicht teilt, teilt es $y - y'$. Also $y \equiv y' \pmod{n}$ und so $y = y'$. Wir merken an, daß wenn n keine Primzahl ist, so existieren Zahlen x, x' mit $0 < x, x' < n$ und $x \cdot x' \equiv 0 \pmod{n}$, also $x \odot_n x' = 0$.

Ein Paar $\mathfrak{G} = \langle E, K \rangle$, wo E eine beliebige, nichtleere Menge ist und $K \subseteq \binom{E}{2}$, heißt ein **Graph**. Falls nichts anderes gesagt wird, ist E endlich, und damit ist natürlich auch K endlich. E ist die Menge der **Ecken** und K die Menge der **Kanten** des Graphen. Eine Kante ist also nichts anderes als eine Paarmenge $\{u, v\} \subseteq E$. Wir schreiben oft uv (oder vu) für die Kante $\{u, v\}$. Wir sagen, u und v seien **benachbart** oder **adjazent** (in $\mathfrak{G}$), falls $uv \in K$. Ist ferner $u \in k$, $k \in K$, so heißt u mit k **inzident**. Zwei Kanten k und ℓ heißen **inzident**, falls $k \cap \ell \neq \emptyset$, das heißt, wenn sie eine gemeinsame Ecke haben. Ein paar Beispiele für Graphen.

Beispiel 1. Sei $K = \binom{n}{2}$. Dann heißt der Graph **vollständig**. Ist $\sharp E = n$, so bezeichnet man diesen Graphen mit K_n.

Beispiel 2. Sei $E = S \cup T$, wobei $S \cap T = \emptyset$. Ferner bestehe jede Kante aus je einem Element aus S und einem Element aus T. Dann heißt der Graph **bipartit**. Er heißt vollständig bipartit, falls $K = \{\{u, v\} : u \in S, v \in T\}$. Ist $\sharp S = m$ und $\sharp T = n$, so bezeichnen wir den Graphen mit $K_{m,n}$.

Beispiel 3. Sei $E = \{e_1, e_2, \ldots, e_n\}$, und $K = \{\{e_i, e_{i+1}\} : 0 < i < n\}$. Dieser Graph heißt **linearer Graph der Länge** $n - 1$.

Beispiel 4. Sei $E = \{e_1, e_2, \ldots, e_n\}$ und $K = \{\{e_i, e_{i+1}\} : 0 < i < n\} \cup \{\{e_n, e_1\}\}$. Dieser Graph heißt schlicht ein **Kreis** der **Länge** $n-1$. (Wir können auch schreiben $K = \{\{e_i, e_j\} : j \equiv i + 1 \pmod{n}\}$.)

Beispiel 5. Es sei E die Menge der Folgen der Länge n über $\{0,1\}$. Es sei $d(\vec{x},\vec{y}) := \sharp\{i : x_i \neq y_i\}$ der sogenannte **Hammingabstand** von $\vec{x}$ und $\vec{y}$. Betrachte $K = \{\{\vec{x},\vec{y}\} : d(\vec{x},\vec{y}) = 1\}$. Dieser Graph heißt **(Hyper–)Würfel der Dimension** n. Für $n = 2$ ist dies genau ein Quadrat, für $n = 3$ genau der allbekannte Würfel.

Beispiel 6. Der **Petersen–Graph** sieht wie folgt aus. Es ist $E = E_i \cup E_a$, wobei $E_i = \{i_0, i_1, \ldots, i_4\}$ und $E_a = \{a_0, a_1, \ldots, a_4\}$. $K = K_a \cup K_{ia} \cup K_i$, wobei $K_a = \{\{i_m, i_n\} : m \equiv n+1 \pmod 5\}$, $K_{ia} = \{\{i_k, a_k\} : 0 \leq i < 5\}$ und $K_i = \{\{i_p, i_q\} : q \equiv p+2 \pmod 5\}$. Man kann sich den Petersen–Graph so vorstellen: $\langle E_i, K_i\rangle$ ist der sogenannte *Drudenfuß*, dem ein Fünfeck $\langle E_a, K_a\rangle$ umschrieben wird.

Zwei Graphen $G = \langle E, K\rangle$ und $H = \langle F, L\rangle$ heißen **isomorph**, falls es eine bijektive Abbildung $h : E \to F$ gibt, derart, daß für alle $u, v \in E$ gilt $uv \in K$ genau dann, wenn $h(u)h(v) \in L$. (Wir können dies etwas prägnanter ausdrücken. Es bezeichne $h[K] := \{\{h(u), h(v)\} : uv \in K\}$. Dann verlangen wir $h[K] = L$.) Es sind alle vollständigen Graphen mit gleicher Eckenzahl isomorph. Dies haben wir schon in der Schreibweise K_n zum Ausdruck gebracht; diese drückt lediglich eine Abhängigkeit von $n = \sharp E$ und nicht von E aus. Ebenso ist für den Isomorphietyp eines vollständigen bipartiten Graphen lediglich die Mächtigkeit der Mengen S und T ausschlaggebend.

Definition 0.69 *Es sei $\mathfrak{G} = \langle E, K\rangle$ ein Graph und u eine Ecke von $\mathfrak{G}$. Dann heißt $N(u) := \{v : uv \in K\}$ die Menge der* ***Nachbarn*** *von u. Für $S \subseteq E$ sei $N(S) := \{v : uv \in K$ für ein $u \in S\}$. Ferner ist $d(u) := \sharp N(u)$ der* ***Grad*** *von u. Ist $d(u) = 0$, so heißt u* ***isoliert****. $N^k(S)$ für $S \subseteq E$ sei wie folgt definiert.*

$$\begin{array}{lcl} N^0(S) & := & S \\ N^{k+1}(S) & := & N^k(S) \cup N(N^k(S)) \end{array}$$

$Z(S) := \bigcup_i N^i(S)$ heißt die ***Zusammenhangskomponente*** *von S. $\mathfrak{G}$ heißt* ***zusammenhängend****, falls $E = Z(\{x\})$ für ein $x \in E$ gilt.*

Es ist $N^k(S)$ die Menge aller Ecken, die von einer Ecke aus S in höchstens k Schritten erreichbar sind. Für endliche Graphen gilt: es existiert ein k dergestalt, daß $Z(S) = N^k(S)$ ist für alle k.

Definition 0.70 *Es sei $G = \langle E, K\rangle$ ein Graph und $S \subseteq E$. Dann sei $d(S)$ die kleinste Zahl derart, daß mit $E = N^d(S)$. Falls diese nicht existiert, so setze $d(S) := \infty$. Der* **Durchmesser** *von G ist*

$$d(G) := \max_{S \subseteq E} d(S)$$

Falls G endlich, so ist $d(G)$ endlich genau dann, wenn G zusammenhängend ist. Dann ist sogar $d(G) < \sharp E$.

Satz 0.71 *In einem endlichen Graphen gilt stets*

$$\sum_{u \in E} d(u) = 2 \cdot \sharp K$$

Beweis. Die linke Summe zählt alle Paare $\langle u, v\rangle$ derart, daß $uv \in K$. Da nun stets $u \neq v$ gilt, wenn $uv \in K$, so entspricht jeder Kante genau zwei Paaren. Q. E. D.

Satz 0.72 *In jedem Graphen ist die Anzahl der Ecken ungeraden Grades eine gerade Zahl.*

Beweis. Sei E_u die Menge der Ecken, für die $d(u)$ ungerade ist, und E_g die Menge aller Ecken, für die $d(u)$ gerade ist. Dann ist nach dem vorigen Satz $2 \cdot \sharp K = \sum_{u \in E} d(u) = \sum_{u \in E_u} d(u) + \sum_{u \in E_g} d(u)$. Es ist $\sum_{u \in E_g} d(u)$ stets gerade, also ist auch $\sum_{u \in E_u} d(u)$ gerade. Dann ist E_u gerade. Das war zu zeigen. Q. E. D.

Es sei nun als erstes ein Satz gezeigt, der gewissermaßen die erste Anwendung der Graphentheorie überhaupt darstellt, nämlich die Lösung des Königsberger Brückenproblems. In abstrakter Form dargestellt, lautet es so: *existiert eine Folge $F = k_1 k_2 \ldots k_r$ von Kanten aus K derart, daß jede Kante aus K genau einmal auftritt, und so daß k_i mit k_{i+1} für $1 \leq i < r$ und k_r mit k_1 jeweils inzident sind*? Eine solche Folge heißt ein **Euler–Zug**. Ferner verabreden wir, eine Folge $u_1 u_2 \ldots u_r$ von Ecken einen **Weg** der Länge $r - 1$ zu nennen, wenn $u_i u_{i+1} \in K$ für alle $1 \leq i < r$. Ein Weg ist **geschlossen**, falls $u_r = u_1$. Ist F ein Euler–Zug, so definiert dieser einen eindeutig bestimmten Weg. Denn seien $k_i k_{i+1}$ zwei aufeinanderfolgende Kanten aus F, dann hat $k_i \cap k_{i+1}$ genau ein Element. Es sei also u_{i+1} das eindeutig bestimmte v mit $v \in k_i \cap k_{i+1}$, und es sei u_1 das eindeutig bestimmte v mit $k_1 = vu_2$, u_{r+1} das eindeutig bestimmte v mit $k_r = u_r v$. Wir nennen einen Weg **nichtwiederholend**, falls $u_i = u_j$ nur dann gilt wenn $i = j$ oder $\{i, j\} = \{1, r\}$. Ein nichtwiederholender, geschlossener Weg heiße **Kreis**.

Satz 0.73 *In einem Graphen existiert ein Euler–Zug genau dann, wenn der Graph zusammenhängend ist und keine Ecke einen ungeraden Grad hat.*

Beweis. Die Bedingungen sind notwendig. Denn wenn $\mathfrak{G}$ nicht zusammenhängend ist, gibt es keine Ecke, von der aus alle Ecken erreichbar sind. Ferner: ist W ein Euler–Zug der Länge r, so ist u_i, $1 < i \leq r$, stets inzident mit $u_i u_{i+1}$ und $u_{i-1} u_i$ (und diese Kanten sind verschieden). Genauso ist u_{r+1} mit $u_1 u_{r+1}$ und $u_r u_{r+1}$ inzident. Jede Ecke ist also mit einer geraden Anzahl Kanten inzident. Nun also zur Umkehrung. Zunächst einmal zeigen wir: in einem Graphen, in dem jede Ecke geraden Grad hat, existiert ein Kreis durch einen gegebene Ecke. Sei u_1 also gegeben. Wir wählen eine beliebige zu u_1 adjazente Ecke u_2. Sei $\mathfrak{G}_1 := \langle E, K - \{\{u_1, u_2\}\}\rangle$. In $\mathfrak{G}_1$ haben u_1 und u_2 ungeraden Grad. Also existiert eine zu u_2 adjazente Ecke u_3. Es gilt $u_3 \neq u_1$ (sowie auch $u_3 \neq u_2$). Induktiv definieren wir eine Folge u_i, derart daß $u_1 u_2 \ldots u_i$ ein nichtwiederholender Weg ist. Ferner setzen wir

$$\mathfrak{G}_i := \langle E, K - \{\{u_i, u_{i+1}\} : 1 \leq j < i\}\rangle$$

Ist $u_i \neq u_1$, so hat u_i einen ungeraden Grad in $\mathfrak{G}_i$. (Denn wir haben aus $\mathfrak{G}$ genau eine mit u_i inzidente Kante entnommen.) Also existiert in $\mathfrak{G}_i$ eine zu

u_i inzidente Ecke u_{i+1}. Ist $u_{i+1} = u_j$ für ein $j \leq i$, so gilt sicher $j < i - 1$. Also haben wir einen Kreis. Ist andererseits u_{i+1} verschieden von allen u_j, so ist $u_1 u_2 \ldots u_{i+1}$ ein nichtwiederholender Weg. Nun haben wir zwar noch nicht gezeigt, daß ein Kreis durch u_1 existiert, aber wir können aus K nun die Kantenmenge des eben konstruierten Kreises entfernen und erhalten so einen Graphen, in dem jede Ecke einen geraden Grad hat, und insbesondere ist der Grad von u_1 nicht Null ist (da wir keine mit u_1 inzidente Kante entnommen haben). Nun machen wir das gleiche Spiel nochmal mit dem neuen Graphen. Es ist klar, daß bei diesem Wegnehmen jede Kante einmal drankommt. Also ist u_1 in einem Kreis, da es in einer Kante ist. Dies zeigt unsere erste Behauptung. Der Satz folgt nun so. Wir wählen einen Kreis K_1 mit Kantenmenge γ_1. $W_1 := K_1$. Dann sei $\mathfrak{G}^1 := \langle E, K - \gamma_1 \rangle$. Da wir zu jedem Punkt genau zwei inzidente Kanten entnehmen, hat in $\mathfrak{G}^1$ jede Ecke geraden Grad. Falls die Kantenmenge noch nicht leer ist, existiert eine Kante in $K - \gamma_1$. Es existiert sogar eine Kante $uv \notin \gamma_1$, derart, daß eine Ecke auf dem Kreis liegt, etwa u. Wir wählen nun in $\mathfrak{G}^1$ einen Kreis K_2 durch u. Nun definieren wir einen neuen Weg wie folgt: wir schieben bei u in K_1 den Kreis K_2 ein. Das Ergebnis ist ein geschlossener Weg W, auf dem keine Kante wiederholt wird. Sei γ_2 seine Kantenmenge. Wir setzen $\mathfrak{G}^2 := \langle E, K - \gamma_2 \rangle$. Wir fahren so fort. Es existiert eine Kante uv, die nicht in γ_2 liegt, aber mit einer Ecke aus W_2 inzident ist. Andernfalls ist $\mathfrak{G}$ nicht zusammenhängend. Q. E. D.

Übungen.

Übung 36. Bestimmen Sie den Durchmesser des n–dimensionalen Würfels und des Petersen–Graphs.

Übung 37. Geben Sie für beliebiges n einen Graphen mit n Ecken an, der den Durchmesser 2 hat, sowie einen Graphen mit Durchmesser $n - 1$.

Übung 38. Es sei $\mathfrak{G}$ ein Grpah ohne isolierte Ecken. Ein Weg in $\mathfrak{G}$ heißt **offener Euler–Zug**, falls alle Kanten genau einmal vorkommen, aber die erste Ecke nicht mit der letzten Ecke übereinstimmt. Zeigen Sie: genau dann gibt es in einem Graphen einen offenen Euler–Zug, wenn der Graph zusammenhängend ist und genau zwei Ecken einen ungeraden Grad haben. *Hinweis.* Da ist also gerade die Verallgemeinerung des Problems vom Haus des Nikolaus. Führen Sie dieses durch einen kleinen Trick auf Satz 0.73 zurück. Seien nämlich u und v genau die Ecken mit ungeradem Grad. Dann füge man zu dem Graphen die Kante uv hinzu. Dann geht alles wir gewünscht (beweisen!). Einzige Schwierigkeit: es kann sein, daß uv schon Kante des Graphen ist (wie beim Haus des Nikolaus). In diesem Fall muß man wieder einen kleiner Trick anwenden, der hier aber nicht verraten wird.

Übung 39. Zeigen Sie: genau dann ist $\mathfrak{G} = \langle E, K \rangle$ unzusammenhängend, wenn es zwei Mengen A und B gibt derart, daß $E = A + B$, $A \cap B = \emptyset$, und $K \subseteq \binom{A}{2} \cup \binom{B}{2}$.

Übung 40. Es habe $\mathfrak{G}$ keine isolierten Ecken. Zeigen Sie, daß $\mathfrak{G}$ genau dann

zusammenhängend ist, wenn es einen geschlossenen Weg gibt, der jede Kante mindestens einmal enthält. *Hinweis.* Dieser Weg muß kein Euler–Zug sein!

Teil 9. Graphen II. Konstruktionen und Darstellung.

Sei $\mathfrak{G} = \langle E, K\rangle$. Ohne Beschränkung der Allgemeinheit ist $E = \{1, 2, \ldots, n\}$. Dann können wir $\mathfrak{G}$ die folgende **Inzidenzmatrix** $I(\mathfrak{G})$ zuordnen. Es ist $I(\mathfrak{G}) := (a_{ij})_{ij}$, wobei $a_{ij} = 1$ genau dann, wenn $\{i, j\} \in K$ und $a_{ij} = 0$ sonst. Die Inzidenzmatrix ist symmetrisch, das heißt, es ist $a_{ij} = a_{ji}$ für alle i, j. Jede $n \times n$–Matrix $A = (a_{ij})_{ij}$ ist eine Inzidenzmatrix eines Graphen über $\{1, 2, \ldots, n\}$, falls für alle i, j mit $1 \leq i, j \leq n$ (i) $a_{ij} \in \{0, 1\}$, (ii) $a_{ii} = 0$, und (iii) $a_{ij} = a_{ji}$. Die Inzidenzmatrix eines vollständigen Graphen besteht nur aus Einsen, die Inzidenzmatrix eines Kreises ist eine Permutationsmatrix. Ferner ist die Inzidenzmatrix eines bipartiten Graphen bis auf Umbenennung von den Elementen von der Form

$$\begin{pmatrix} \mathbf{0} & A \\ B & \mathbf{0} \end{pmatrix}$$

wobei $\mathbf{0}$ für die Nullmatrix entsprechender Größe steht, und A und B beliebige Matrizen sind. Im Falle des vollständigen bipartiten Graphen sind $A = \mathbf{1}$ und $B = \mathbf{1}$, wobei $\mathbf{1}$ wieder für die Matrix aus Einsen der entsprechenden Größe steht.

Mit Hilfe der Inzidenzmatrix kann man folgende interessante Beziehung festhalten.

Satz 0.74 *Es sei $I^k(\mathfrak{G}) = (c_{ij})_{ij}$ das k–fache Produkt von $I(\mathfrak{G})$ mit sich selbst, $k > 0$. Dann ist c_{ij} genau die Anzahl der Wege der Länge k von i nach j.*

Beweis. Induktion über k. Es ist $I^1(\mathfrak{G}) = I(\mathfrak{G}) = (a_{ij})_{ij}$, und ein Weg der Länge 1 genau eine Kante. Die Behauptung ist in diesem Falle also richtig. Nun sei $I^k(\mathfrak{G}) = (c_{ij})_{ij}$ und $I^{k+1}(\mathfrak{G}) = (d_{ij})_{ij}$. Dann ist $d_{ij} = \sum_{r=1}^{n} c_{ir} \cdot a_{rj}$. Die rechte Summe erstreckt sich über die Anzahl der Wege von i nach r, für die eine Kante von r nach j existiert, $1 \leq r \leq n$. Dies ist aber gerade die Anzahl der Wege der Länge $k + 1$ von i nach j. Q. E. D.

Ist $\mathfrak{G} = \langle E, K\rangle$ Graph, $F \subseteq E$, so setze $L := K \cap \binom{F}{2}$. Das Paar $\langle F, L\rangle$ heißt der von $\mathfrak{G}$ auf F **induzierte Graph**. Ist zum Beispiel $\mathfrak{G}$ vollständig, so ist jeder induzierte Teilgraph auch vollständig. Ist $L \subseteq K \cap \binom{F}{2}$, so heißt $\langle E, L\rangle$ **Teilgraph** von $\mathfrak{G}$. Sei ferner $h : E \twoheadrightarrow F$ eine surjektive Abbildung derart, daß der von $h^{-1}(x)$ induzierte Teilgraph zusammenhängend ist für jedes $x \in F$. Nun sei $L := h[K] \cap \binom{F}{2}$. Das Paar $\langle F, L\rangle$ heißt dann eine **Kontraktion** von $\mathfrak{G}$. Es gilt nun folgendes

Satz 0.75 *Es sei $\mathfrak{G}$ eine Kontraktion von $\mathfrak{H}$. Dann ist $\mathfrak{G}$ genau dann zusammenhängend, wenn $\mathfrak{H}$ zusammenhängend ist.*

Zum Beweis zeigen wir als erstes folgendes. Eine Kontraktion heiße **elementar**, falls es ein $x \in F$ gibt mit $h^{-1}(x) \in K$ und für alle $y \neq x$ hat $h^{-1}(y)$ genau ein Element. Intuitiv gesprochen kontrahieren wir bei einer elementaren Kontraktion eine Kante. Es ist nicht schwer zu sehen, daß jede Kontraktion eine

Verkettung von elementaren Kontraktionen ist. Also muß man obenstehenden Satz nur für elementare Kontraktionen zeigen. Dies ist nicht schwer.

Bevor wir dies tun, werden wir uns noch überlegen, daß man eine elementare Kontraktion auch etwas anders beschreiben kann. Es sei $\mathfrak{G} = \langle E, K\rangle$ gegeben und $uv \in K$. Das Resultat der Kontraktion von uv ist der folgende Graph $\mathfrak{H} = \langle E - \{v\}, L\rangle$, wobei

$$L := K \cap \binom{E - \{v\}}{2} \cup \{ux : x \in E - \{u, v\}, xv \in K\}$$

Das heißt, wir nehmen den auf $E - \{v\}$ induzierten Graphen und fügen alle Kanten ux hinzu, für die $xv \in K$.

Sei nun $\mathfrak{G}$ unzusammenhängend. Dann existieren Mengen A, B mit $A \cup B = E$, A und B disjunkt und $K \subseteq \binom{A}{2} \cup \binom{B}{2}$. Ist $uv \in K$, so ist ohne Beschränkung der Allgemeinheit $uv \in \binom{A}{2}$. Wir behaupten: ist $\mathfrak{H} = \langle E - \{v\}, L\rangle$ das Ergebnis der Kontraktion von uv, so ist jede Kante von $\mathfrak{H}$ entweder in $\binom{A-\{v\}}{2}$ oder in $\binom{B}{2}$. Sei nämlich $xy \in L$ eine Kante. Ist $x \in B$, so ist nach Definition von L $y \in B$. Also ist $L \subseteq \binom{A-\{v\}}{2} \cup \binom{B}{2}$, dh $\mathfrak{H}$ unzusammenhängend, wie versprochen. Sei umgekehrt $\mathfrak{H}$ unzusammenhängend, etwa $L \subseteq \binom{A}{2} \cup \binom{B}{2}$ für disjunkte Mengen A, B. Es sei $E = A \cup B \cup \{v\}$. Ferner existiert in $\mathfrak{G}$ eine Kante uv. Daher ist $u \in A$ oder $u \in B$. Ohne Beschränkung der Allgemeinheit $u \in A$. Wir setzen $A' := A \cup \{v\}$ und $B' := B$. Wir behaupten, daß $K \subseteq \binom{A'}{2} \cup \binom{B'}{2}$. Dazu sei $xy \in K$. Falls xy nicht mit uv inzident ist, so ist $xy \in \binom{A}{2}$ oder $xy \in \binom{B}{2}$ und wir sind fertig. Andernfalls ist $x = u$ oder $x = v$. (Der Fall $y = u$ oder $y = v$ ist ganz analog.) Sei $x = u$. Ist $y = v$, so ist ja $y \in A'$ und so $xy \in \binom{A'}{2}$. Ist $y \neq v$, so ist $xy \in L$; also $xy \in \binom{A}{2} \subseteq \binom{A'}{2}$. Sei nun $x = v$. Der Fall $y = v$ braucht nicht betrachtet zu werden. Sei also zusätzlich $y \neq v$. Dann ist $uy \in L$, also $y \in A'$. Daraus folgt $uy \in \binom{A}{2}$, und so $xy \in \binom{A'}{2}$. Daher ist $\mathfrak{G}$ unzusammenhängend.

Definition 0.76 *$\mathfrak{H}$ ist ein* ***Minor*** *von $\mathfrak{G}$, falls $\mathfrak{H}$ Kontraktion eines Teilgraphen von $\mathfrak{G}$ ist.*

Die Relation *ist Minor von* ist transitiv, wie aus dem folgenden Satz folgt.

Satz 0.77 *Ist $\mathfrak{I}$ Teilgraph oder Kontraktum von $\mathfrak{H}$ und ist $\mathfrak{H}$ Minor von $\mathfrak{G}$, so ist $\mathfrak{I}$ Minor von $\mathfrak{G}$.*

Beweis. Es sei $\mathfrak{G} = \langle E, K\rangle$ und $\mathfrak{H} = \langle P, Q\rangle$. Nach Voraussetzung existiert ein $F \subseteq E$ und eine Abbildung $h : F \twoheadrightarrow P$ derart, daß $Q \subseteq h[K] \cap \binom{F}{2}$. Nun sei $\mathfrak{I} = \langle R, T\rangle$ Kontraktum von $\mathfrak{H}$. Dann existiert $g : P \twoheadrightarrow R$ mit $T = g[Q]$. Dann ist $T = g[Q] \subseteq (g \circ h)[K] \cap \binom{F}{2}$, also $g \circ h$ eine Kontraktion eines Teilgraphen von $\mathfrak{G}$ auf $\mathfrak{I}$. Sei nun $\mathfrak{I}$ Teilgraph von $\mathfrak{H}$, also $R \subseteq P$ und $T = Q \cap \binom{R}{2}$. Wähle $F := h^{-1}[T]$ und $L := \{uv \in K : h(u)h(v) \in T\}$. Dann ist $\langle F, L\rangle$ nach Konstruktion ein Teilgraph von $\mathfrak{G}$. Ferner ist $h \restriction F : F \twoheadrightarrow R$ und $h[L] = R \cap \binom{R}{2}$. Q. E. D.

Ein Graph heißt **planar** wenn er sich in der Ebene zeichnen läßt, ohne daß die Kanten sich überschneiden. Planare Graphen sind aus vielen Gründen

sehr interessant. Das Vier–Farben–Problem bezieht sich auf planare Graphen (Landkarten); aber auch in der Elektronik sind sie von immenser Wichtigkeit. Man denke nur an Schaltkreise. Die Leiterbahnen in Schaltkreisen entsprechen den Kanten eines Graphen, dessen Ecken gerade die Schaltelemente sind. Falls sich Kanten schneiden, so muß man auf der Platine eine sogenannte Brücke einbauen. Hochintegrierte Schaltkreise (VSLI) erlauben zwar auch Brücken, jedoch gilt es, so wenig wie möglich davon zu benützen, da sie schwierig zu realisieren sind — also teuer. Planare Graphen sind der Idealfall: man benötigt überhaupt keine Brücken. Wir teilen ohne Beweis den folgenden Sachverhalt mit.

Satz 0.78 (Kuratowski) *Genau dann ist $\mathfrak{G}$ planar, wenn weder $K_{3,3}$ noch der vollständige Graph K_5 ein Minor von $\mathfrak{G}$ sind.*

Wir können jedoch ein paar einfache Überlegungen machen. Eine **Realisierung** von $\mathfrak{G}$ ist ein Paar $\langle p, \ell\rangle$, wo $p : E \to \mathbb{R}^2$ eine Abbildung der Ecken in die reelle Ebene, und für jedes $k = uv \in K$ ist $\ell(k) : [0,1] \to \mathbb{R}^2$ eine stetige Abbildung mit $\ell(k)(0) = u$ und $\ell(k)(1) = v$. Diese Realisierung ist **schnittfrei**, falls es keine Ecken k und k' mit $k \neq k'$ und keine r, r' mit $0 < r, r' < 1$ derart, daß $\ell(k)(r) = \ell(k')(r')$. $\mathfrak{G}$ is nach Definition planar genau dann, wenn es eine schnittfreie Realisierung gibt. Es gilt nun folgendes.

Satz 0.79 *Es sei $\mathfrak{H}$ ein Minor von $\mathfrak{G}$. Ist dann $\mathfrak{G}$ planar, so ist es auch $\mathfrak{H}$.*

Beweis. Sei $\mathfrak{H} = \langle F, L\rangle$ ein Teilgraph von $\mathfrak{G} = \langle E, K\rangle$. Sei $\langle p, \ell\rangle$ eine Realisierung von $\mathfrak{G}$. Dann ist $\langle p \restriction F, \ell \restriction L\rangle$ eine Realisierung von $\mathfrak{H}$ und schnittfrei, falls $\langle p, \ell\rangle$ schnittfrei ist. Für Kontraktionen muß man sich etwas mehr Mühe geben. Da der Beweis relativ trickreich ist, werden wir ihn nicht ausführen. Q. E. D.

Im Übrigen ist jeder Graph schnittfrei im Raum realisierbar.

Definition 0.80 *Seien $\mathfrak{G} = \langle E, K\rangle$ und $\mathfrak{H} = \langle F, L\rangle$ Graphen. Die* ***disjunkte Vereinigung*** *wird definiert durch $\mathfrak{G} + \mathfrak{H} := \langle P, Q\rangle$, wobei*

$$\begin{array}{rcl} P & := & E \times \{0\} \cup F \times \{1\} \\ Q & := & \{\{\langle u, 0\rangle, \langle v, 0\rangle\} : uv \in K\} \cup \{\{\langle u, 1\rangle, \langle v, 1\rangle\} : uv \in L\} \end{array}$$

$\mathfrak{G} + \mathfrak{H}$ zerfällt in (mindestens) zwei Komponenten, zwischen denen keine Kante existiert und die isomorph zu $\mathfrak{G}$ und $\mathfrak{H}$ sind.

Definition 0.81 *Eine* ***Clique*** *in einem Graphen ist eine maximale Menge von Ecken, auf denen der induzierte Graph vollständig ist.*

Offensichtlich ist jede Ecke in einer Clique enthalten. Denn im schlimmsten Fall, wenn u isoliert ist, ist $\{u\}$ schon eine Clique. Es ist ferner so, daß Cliquen sich überschneiden können. In einem Kreis bilden je zwei benachbarte Punkte eine Clique, mit Ausnahme des Kreises aus drei Punkten. Betrachten wir das Problem, eine Landkarte so zu färben, daß je zwei benachbarte Länder nicht dieselbe Farbe erhalten. Dabei gelten zwei Länder als benachbart, falls sie eine

gemeinsame Grenze aus mehr als einem Punkt haben. Eine solche Färbung solle *gut* heißen. Wir können dies graphentheoretisch so deuten. Jedes Land sei eine Ecke, und eine Kante ist ein Paar Länder, welche eine gemeinsame Grenze haben. Offensichtlich entspricht nun einer guten Färbung eine Färbung des zugehörigen Graphen, in welchen Punkte auf einer Kante jeweils unterschiedliche Farben haben. Dies ist gleichbedeutend damit, daß in jeder Clique alle Punkte unterschiedliche Farbe haben. Wir können dies auch so deuten. Eine Färbung mit n Farben ist ja nichts weiter als eine Partition der Eckenmenge in n Mengen. Eine Partition heiße **gut**, falls jede Clique in eine Partitionsmenge in höchstens einem Punkt schneidet. Die kleinste Zahl, für die eine gute Partition der Eckenmenge existiert, heißt die **chromatische Zahl** des Graphen und wird mit $\chi(G)$ bezeichnet. Das Vierfarbensatz lautet nun wie folgt:

Für jeden planaren Graphen G ist $\chi(G) \leq 4$.

Daß dies eine adäquate Formulierung ist, muß man sich allerdings überlegen. Denn man muß zeigen, daß jedem planaren Graphen eine Landkarte zugeordnet werden kann und jeder Landkarte ein planarer Graph. Das ist nicht schwer, wollen wir jedoch nicht tun. Aus dem Satz von Kuratowski folgt übrigens, daß in einem planaren Graphen keine Clique mehr als vier Element hat; dies macht die Behauptung zumindest plausibel. Bewiesen wurde dieser Satz allerdings erst in den siebziger Jahren mit Hilfe eines Computers! Der Beweis ist (bis jetzt) sehr aufwendig. Wir zeigen folgenden einfachen Satz:

Satz 0.82 *Es sei $G = \langle E, K \rangle$ ein endlicher Graph und γ das Maximum aller $d(u)$, $u \in E$. Dann gilt $\chi(G) \leq \gamma + 1$.*

Beweis. Es sei $E = \{x_i : 1 \leq i \leq n\}$. Wir wählen nun induktiv eine Farbe für die x_i. x_1 bekommt eine beliebige Farbe. Seien x_1,..., x_j bereits gefärbt, so betrachten wir x_{j+1}. x_{j+1} hat höchstens γ viele Nachbarn. Nicht alle von ihnen sind bereits gefärbt. In jedem Fall gibt es aber eine Farbe f, welche kein Nachbar von x_{j+1} hat. Wir geben daher x_{j+1} die Farbe f. Offensichtlich läßt sich auf diese Weise der gesamte Graph färben. Q. E. D. Der in dem Beweis verwendete Algorithmus ist ein Beispiel für einen sogenannten *Greedy* Algorithmus. Bei einem solchen Algorithmen wählt man immer die lokal beste Lösung, und dennoch wird am Ende eine global optimale Lösung erreicht. Ein weiteres Beispiel für einen Greedy–Algorithmus ist der Algorithmus zur Bestimmung eines Huffmann–Codes (siehe Teil 12).

Übungen

Übung 41. Es bezeichne W_n den Hyperwürfel der Dimension n. Zeigen Sie: W_n ist induzierter Teilgraph von W_{n+1}. Ebenso ist W_n auch Kontraktum von W_{n+1}.

Übung 42. In der Definition der Kontraktion wurde verlangt, daß der von $h^{-1}(x)$ induzierte Teilgraph zusammenhängend ist für jedes $x \in F$. Wir wollen sehen, was passiert, wenn dies Bedingung fallengelassen wird. Dazu sei eine

schwache Kontraktion von $\langle E, K\rangle$definiert als ein Paar $\langle F, L\rangle$ derart, daß ein $h : E \twoheadrightarrow F$ existiert mit $L = h[K]$. Zeigen Sie: jeder zusammenhängende Graph mit mindestens zwei Ecken ist schwache Kontraktion eines Kreises. *Hinweis.* Wählen Sie einen beliebigen geschlossenen Weg $u_1u_2 \dots u_r$ in $\mathfrak{G}$, der alle Kanten mindestens einmal durchläuft. Da $\mathfrak{G}$ zusammenhängend ist, existiert solch ein Weg (das müssen Sie nicht zeigen). Setzen Sie $F := \{1, 2, \dots, r\}$. Nun muß man L so definieren, daß $\langle F, L\rangle$ ein Kreis ist, und eine Kontraktion $h : F \twoheadrightarrow E$ finden.

Übung 43. Es heiße $\mathfrak{G}$ **lose**, falls jede Ecke den Grad 1 hat. Zeigen Sie: jeder zusammenhängende Graph mit mindestens zwei Ecken ist schwache Kontraktion eines losen Graphen. *Hinweis.* Verwenden Sie die vorige Aufgabe.

Übung 44. Zeigen Sie: der dreidimensionale Hyperwürfel ist planar, der vierdimensionale ist es nicht. *Hinweis.* Für die letzte Behauptung wähle man eine beliebige Ecke, etwa $P_1 := (0, 0, 0, 0)$. Diese hat vier Nachbarn Q_1, Q_2, Q_3 und Q_4. Zu je zwei Q_j und Q_k existiert ein gemeinsamer Nachbar R_{jk} verschieden von P_1. Wähle R_{12}, R_{13}, R_{23} und R_{24}. Zeige nun: $K_{3,3}$ ist ein Minor des Teilgraphen definiert auf diesen Ecken.

Übung 45. Zeigen Sie: der Hyperwürfel der Dimension n ist bipartit für jedes n. *Hinweis.* Betrachten die Menge aller Ecken $\vec{x}$ mit $d(\vec{x}, \vec{0})$ gerade.

Teil 10. Graphen III. Matchings.

Definition 0.83 *Es sei $\mathfrak{G} = \langle S+T, K\rangle$ ein bipartiter Graph. Ein* ***Matching*** *ist eine Menge $L \subseteq K$ derart, daß jede Ecke mit höchstens einer Kante aus L inzident ist.*

Alternativ dazu ist ein Matching ein Teilgraph $\langle S + T, L\rangle$, bei dem jede Ecke höchstens den Grad 1 hat. Die **Matching–Zahl** $m(\mathfrak{G})$ ist die maximale Anzahl aller Kanten eines möglichen Matchings von $\mathfrak{G}$. Ein Matching heißt ein **Maximum–Matching**, falls die Anzahl der Kanten gerade $m(\mathfrak{G})$ ist. Wir fragen uns nun, wann die Matching–Zahl gerade $\sharp S$ ist. In diesem Fall nennen wir das Matching **ideal**. Ist dann $\sharp S = \sharp T$, so ist dann auch jedes Element von T mit jedem Element aus S gematcht. Es muß ideale Matchings nicht geben (zum Beispiel wenn $\sharp S \neq \sharp T$). Wann es sie gibt, dazu gibt es ein schönes Kriterium, bekannt auch unter dem Namen *Heiratssatz.* Wir betrachten dazu eine Kante als ein mögliches Heiratspaar. Bei der gegenwärtigen Rechtslage entsteht dann aus einer beliebigen Menge von Menschen ein bipartiter Graph. Ein Matching entspricht dann einer Auswahl aus den möglichen Heiratspaaren dergestalt, daß jeder einen Partner bekommt. In diesem Gewand ist vielleicht eher klar, warum es ideale Matchings nicht geben muß.

Sei $A \subseteq S$. Dann ist $N(A) \subseteq T$. $N(A)$ war definiert als $\{v : uv \in K$ für ein $u \in A\}$.

Satz 0.84 *Sei $\langle S + T, K\rangle$ ein bipartiter Graph. Genau dann ist $m(\mathfrak{G}) = \sharp S$, wenn $\sharp A \leq \sharp N(A)$ ist für alle $A \subseteq S$.*

Beweis. Zunächst einmal überlegen wir, daß die Bedingung notwendig ist. Dazu sei L ein Matching mit $\sharp L = \sharp S$. Dann existiert zu jedem $u \in S$ genau ein $v \in T$ mit $uv \in L$. Bezeichne v mit $f_L(u)$. Dann ist $f_L : S \to T$ eine injektive Abbildung nach Definition eines Matchings. Also ist, da ja $N(A) \supseteq f_L[A]$ und $\sharp f_L[A] = \sharp A$, $\sharp N(A) \geq \sharp A$. Nun zu der Behauptung, daß die Bedingung auch hinreicht. Sei ein Matching L gegeben mit $\sharp L < \sharp S$. Wir zeigen: es gibt ein Matching M mit $\sharp M > \sharp L$. Es existiert ein $u(0) \in S$ dergestalt, daß $u(0)$ zu keiner Kante aus L inzident ist. Immerhin existiert aber wegen $\sharp N(\{u(0)\}) \geq 1$ ein $v(1) \in T$ mit $u(0)v(1) \in K$. Angenommen, $v(1)$ ist nicht gematcht in L. Dann ist $M := L \cup \{u(0)v(1)\}$ ein Matching mit $\sharp M > \sharp L$. Sei also $v(1)$ gematcht, etwa sei $u(1)v(1) \in L$. Wiederum ist wegen $\sharp N(\{u(0), u(1)\}) \geq 2$ gesichert, daß ein $v(2) \neq v(1)$ existiert mit $u(1)v(2) \in K$ oder $u(0)v(2) \in K$. Ist $v(2)$ nicht gematcht, so hören wir auf, ansonsten besorgen wir uns ein $u(2)$ mit $u(2)v(2) \in L$. Wir können so fortfahren, bis wir eine nichtgematchte Ecke $v(r) \in T$ finden. Zu jedem $v(i)$ mit $1 \leq i \leq r$ existiert dann nach Konstruktion ein $u(j)$ mit $j < i$ und $u(j)v(i) \in K$. Wir haben also einen Weg $W = v(r), u(j_1), v(j_1), u(j_2), v(j_2), \ldots, u(j_p), v(j_p), u(0)$ mit $j_{p+1} := 0 < j_p < \ldots < j_2 < j_1 < r =: j_0$, wobei jeweils $u(j_a)v(j_a) \in L$ und $u(j_{a+1})v(j_a) \in K - L$. Es sei $Q := \{u(j_{a+1})v(j_a) : 0 \leq a \leq p\}$, $P := \{u(j_a)v(j_a) : 0 < a \leq p\}$. Dann ist $\sharp P = p < p + 1 = \sharp Q$. Setze nun $M := (L - P) \cup Q$. Dies ist ein Matching und $\sharp M > \sharp L$. Q. E. D.

Eine Variante des Matchingproblems ist das Auffinden einer sogenannten *Transversale*.

Definition 0.85 *Es sei $S := \{A_1, A_2, \ldots, A_k\}$ ein Mengensystem. Eine* ***Transversale*** *von S ist einen Menge $M = \{m_1, m_2, \ldots, m_k\}$ der Mächtigkeit i, derart, daß für jedes $j \leq k$ gilt $m_j \in A_j$.*

Man beachte, daß keine Transversale existiert, wenn eine der Mengen leer ist. Dazu eine Interpretation. Wir nennen eine Funktion $f : \{1, 2, \ldots, k\} \to \bigcup S := \bigcup_{j=1}^{k} A_j$ eine **Auswahlfunktion**, falls $f(j) \in A_j$ für all $j \leq k$. Solche Auswahlfunktionen gibt es immer. Wir wollen aber eine Auswahlfunktion haben, bei der $f(i) \neq f(j)$ ist für $i \neq j$. Damit haben wir jedem A_i eindeutig einen Repräsentanten $f(i)$ zugeordnet. Es ist damit allerdings nicht ausgeschlossen, daß $f(i) \in A_j$ für $i \neq j$ ist.

Satz 0.86 *Es sei $S = \{A_1, A_2, \ldots, A_k\}$ ein Mengensystem. Genau dann existiert eine Transversale von S, wenn für jedes $P \subseteq \{1, 2, \ldots, k\}$ gilt $\sharp(\bigcup_{i \in P} A_i) \geq \sharp P$.*

Beweis. Definiere einen bipartiten Graphen wie folgt. S sei wie gegeben, $T := \bigcup S$ und $K := \{\{A_i, x\} : x \in A_i\}$. Dann ist $\mathfrak{S} := \langle S + T, K \rangle$ bipartiter Graph. Eine Transversale S ist dann genau ein Matching von $\mathfrak{S}$ mit Mächtigkeit $\sharp S$. Dies existiert genau dann, wenn zu jedem $P \subseteq S$ gilt $\sharp N(P) \geq \sharp P$. Aber $\sharp N(P) = \{x : x \in \bigcup_{i \in P} A_i\}$. Q. E. D.

Ist zum Beispiel $A_1 = \varnothing$, so ist $\sharp A_1 = 0 < 1$, also existiert laut dem Satz keine Transversale. Wir sind allerdings die Antwort schuldig geblieben, wie groß

im allgemeinen Fall $m(\mathfrak{G})$ ist. Dazu definieren wir den Matching–Defekt eines Graphen.

Definition 0.87 *Es sei $\mathfrak{G} = \langle S+T, K\rangle$ ein bipartiter Graph. Der* ***Matching–Defekt*** *von $\mathfrak{G}$, $\delta(\mathfrak{G})$, ist das Maximum der Anzahlen $\sharp A - \sharp N(A)$ für solche A, wo $\sharp A \geq \sharp N(A)$ ist.*

Da $\sharp\varnothing \geq \sharp N(\varnothing) = \varnothing$, ist der Matching–Defekt immer definiert und Null genau dann, wenn stets $\sharp A \leq \sharp N(A)$. Daher existiert ein Matching mit Mächtigkeit $\sharp S$ genau dann, wenn der Matching–Defekt Null ist.

Satz 0.88 *Es sei $\mathfrak{G} = \langle S + T, K\rangle$ ein bipartiter Graph. Dann ist $m(\mathfrak{G}) = \sharp S - \delta(\mathfrak{G})$.*

Beweis. Gewiß kann in einem Matching L nicht $\sharp L > \sharp S - \delta(\mathfrak{G})$ sein. Denn sei $A \subseteq S$ so gewählt, daß $\sharp A - \sharp N(A) = \delta(\mathfrak{G})$. Dann können höchstens $\sharp A - \delta(\mathfrak{G})$ Ecken aus A gematcht werden. Selbst wenn im günstigsten Fall alle Ecken aus $S - A$ gematcht sind, existieren $\delta(\mathfrak{G})$ ungematchte Ecken. Also $\sharp L \leq \sharp A - \delta(\mathfrak{G}) \leq \sharp S - \delta(\mathfrak{G})$. Wir zeigen nun, daß das Maximum erreicht wird. Dazu sei $T^* := T \cup D$, wobei D eine zu T disjunkte Menge der Mächtigkeit $\delta(\mathfrak{G})$ ist. Ferner sei $K^* := K \cup \{ud : u \in S, d \in D\}$, $\mathfrak{G}^* := \langle S \cup T^*, K^*\rangle$. $\mathfrak{G}^*$ ist ein bipartiter Graph. Es gilt $N^*(A) = N(A) \cup D$. Also ist der Matching–Defekt von $\mathfrak{G}^*$ gleich Null. Daher existiert ein Matching L^* mit $\sharp L^* = \sharp S$. Nun enthält L^* genau $\delta(\mathfrak{G})$ viele Kanten mit einer Ecke aus D. Sei also $L := L^* \cap \binom{S\cup T}{2}$. Dann ist L ein Matching mit $\sharp L = \sharp L^* - \delta(\mathfrak{G}) = \sharp S - \delta(\mathfrak{G})$, wie versprochen. Q. E. D.

Als letztes noch eine andere Charakterisierung der Matching–Zahl. Wir nennen eine Menge $D \subseteq E$ einen **Träger** des Graphen, falls jede Kante aus $\mathfrak{G}$ mit einer Ecke aus D inzident ist. Wir können in einem bipartiten Graphen zum Beispiel $D = S$ wählen oder $D = T$. Daher können Träger durchaus kleiner sein als die Eckenmenge.

Satz 0.89 *In einem bipartiten Graphen $\mathfrak{G}$ gilt:*

$$min\{\sharp D : D \textit{ Träger}\} = max\{\sharp L : L \textit{ Matching}\}$$

Beweis. Setze $\tau(\mathfrak{G}) := min\{\sharp D : D \textit{ Träger}\}$. Es ist $max\{\sharp L : L \textit{ Matching}\} = \sharp S - \delta(\mathfrak{G}) = \sharp S - \sharp A + \sharp N(A)$ für ein gewisses $A \subseteq S$. Setze $D := (S - A) \cup N(A)$. D ist ein Träger von $\mathfrak{G}$. Denn sei $k \in K$, etwa $k = uv$ mit $u \in S$ und $v \in T$. Ist $u \notin A$, dann ist $u \in D$. Ist andererseits $u \in A$, dann ist $v \in N(A)$, also $v \in D$. Es gilt $\sharp D = \sharp S - \sharp A + \sharp N(A)$. (Beachte, daß A und $N(A)$ disjunkt sind.) Also ist $\tau(\mathfrak{G}) \leq m(\mathfrak{G})$. Aber $\tau(\mathfrak{G}) < m(\mathfrak{G})$ kann nicht gelten. Denn jeder Träger von $\mathfrak{G}$ ist auch Träger jeden Matchings von $\mathfrak{G}$. Ein Träger eines Matchings L hat aber mindestens $\sharp L$ Elemente. Q. E. D.

In dieser Formulierung hat dieser Satz die Form eines Minimum–Maximum Prinzips. Solche Prinzipien sind häufig anzutreffen (zum Beispiel auch der Minimum Schnitt–Maximum Fluß–Satz in dem nächsten Kapitel).

Wir beschließen diesen Teil mit einem anschaulichen Beispiel eines bipartiten Graphen.

Definition 0.90 *Eine* ***affine Ebene*** *ist ein Paar $\langle P, G\rangle$, falls P eine Menge ist, die Menge von* ***Punkten****, und $G \subseteq \wp(P)$ die Menge der* ***Geraden****, und ferner gilt: (1) je zwei (verschiedene) Punkte liegen auf genau einer Geraden; (2) zu jeder Gerade g und jedem Punkt $Q \notin g$ existiert genau eine Gerade h mit $Q \in h$ und $g \cap h = \varnothing$; (3) je zwei (verschiedene) Geraden schneiden sich in höchstens einem Punkt; (4) eine Gerade enthält mindestens 3 Punkte; (5) es gibt mindestens drei Geraden. g ist* ***parallel*** *zu h, $g = h$ oder $g \cap h = \varnothing$.*

Wir können eine affine Ebene als bipartiten Graphen schreiben mit $S := P$, $T := G$, und $K := \{Qg : Q \in P, g \in T, Q \in g\}$. Für $Q \in S$ ist $N(Q)$ gerade das sogenannte **Geradenbündel** durch Q.

Satz 0.91 *Es sei $\langle P, G\rangle$ eine affine Ebene. Dann gilt für alle Punkte Q und alle Geraden g: $\sharp N(Q) = \sharp g + 1$. Ferner gilt für alle Punkte Q, Q', daß $\sharp N(Q) = \sharp N(Q')$, und es gilt für je zwei Geraden g, g', daß $\sharp g = \sharp g'$.*

Beweis. Die erste Behauptung zeigt die anderen. Denn es ist für beliebige Punkte Q, Q' und beliebige Geraden g und g', daß $\sharp N(Q) = \sharp g + 1 = \sharp N(Q') = \sharp g' + 1$. Also $\sharp N(Q) = \sharp N(Q')$ sowie $\sharp g = \sharp g'$. Es bezeichne $\overline{QR}$ die Gerade, welche sowohl Q als auch R enthält. Sei $Q \notin g$. Es existiert nun genau eine Gerade $h \in N(Q)$ und $h \cap g = \varnothing$. Dann ist $R \mapsto \overline{QR}$ eine Bijektion zwischen g und $N(Q) - \{h\}$. Nun benötigen wir noch eine Bijektion zwischen g und $N(Q) - \{h\}$ in dem Fall, wo $Q \in g$. In diesem Fall wählen wir $h = g$. Nun wählen einen Punkt $T \notin g$ und nennen f die durch T gehende, zu g parallele Gerade. Ferner sei U ein Punkt nicht auf g oder h und k eine Gerade durch U. Man verschalte nun die Bijektionen $N(Q) - \{g\} \to h \to N(U) - \{k\} \to g$. Q. E. D.

Übungen

Übung 46. Berechne $\delta(\mathfrak{G})$ für den n–dimensionalen Hyperwürfel. Dieser ist nämlich bipartit. Geben Sie auch einen Träger dieses Graphen an.

Übung 47. Berechnen Sie die Anzahl der Elemente eines kleinsten Trägers eines vollständigen Graphen.

Übung 48. Zeigen Sie: in einem Graphen $\mathfrak{G}$ liegt $\tau(\mathfrak{G}) := min\{\sharp D : D\ Träger\}$ irgendwo zwischen 0 und $\sharp E - 1$. Finden Sie Graphen, für die $\tau(\mathfrak{G}) = 0$, 1 beziehungsweise $\tau(\mathfrak{G}) = \sharp E - 1$ ist.

Übung 49. Es sei p eine Primzahl. Betrachte die Menge P aller Paare $\langle x, y\rangle$ von Resten modulo p; diese seien die Punkte. Setze G die Menge aller Mengen von der Form $\{\binom{x_1}{x_2} + \lambda\binom{y_1}{y_2} : 0 \le \lambda < p\}$. Diese seien die Geraden. Zeigen Sie: ist $p > 2$, so ist $\mathbb{F}_p^2 := \langle P, G\rangle$ eine affine Ebene. *Hinweis.* Zeigen Sie in jedem Fall (4) und (5), aber nur eines von (1), (2) und (3). Für Extrapunkte kann man selbstverständlich auch mehr zeigen.

Übung 50. Zeigen Sie, daß der Petersen–Graph nicht bipartit ist. Zeigen Sie ferner, daß es einen Träger aus 6 Ecken gibt. (Dieser ist auch minimal, wie man zeigen kann.)

Teil 11. Graphen IV. Netzwerke und Flüsse.

Definition 0.92 *Ein Paar $\langle E, K\rangle$ heißt* ***gerichteter Graph****, falls E eine nichtleere Menge (die Menge der Ecken) und $K \subseteq E \times E$ eine Menge von Kanten. Ist $k \in K$ und $k = \langle u, v\rangle$, so heißt $k^- := u$ die* ***Anfangsecke*** *und $k^+ := v$ die* ***Endecke*** *von k.*

Zu einer Ecke $u \in E$ setze $N^-(u) := \{v : \langle u, v\rangle \in K\}$ und $N^+(u) := \{v : \langle v, u\rangle \in K\}$. Ebenso ist $N^-(S)$, $N^+(S)$ für $S \subseteq E$ definiert. Der **(Vorwärts–)Transit** von S ist die kleinste Menge T mit $S \subseteq T$ und $T \subseteq N^-(T)$. Analog ist der Rückwärtstransit definiert. Der **Ingrad** von u ist $d^+(u) := \sharp N^+(u)$ und der **Ausgrad** $d^-(u) := \sharp N^-(u)$. Ist der Ingrad von u Null, so heißt u eine **Quelle**; ist der Ausgrad von u gleich Null, so heißt u eine **Senke**.

Satz 0.93 *In einem gerichteten Graphen gilt*

$$\sum_{u \in E} d^+(u) = \sum_{u \in E} d^-(u) = \sharp K$$

Der Beweis ist einfach. Ohne Beschränkung der Allgemeinheit ist $E = \{1, 2, \ldots, n\}$. Falls gilt, daß nicht zugleich $\langle u, v\rangle \in K$ und $\langle v, u\rangle \in K$ für verschiedene u, v, sowie $\langle u, u\rangle \notin K$ für alle $u \in K$, so können wir für $\mathfrak{G}$ können eine $n \times n$–Inzidenzmatrix $J(\mathfrak{G}) = (b_{ij})_{ij}$ definieren durch

$$b_{ij} := \begin{cases} 1 & \text{falls } \langle i, j\rangle \in K \\ -1 & \text{falls } \langle j, i\rangle \in K \\ 0 & \text{falls } \langle i, j\rangle, \langle j, i\rangle \notin K \end{cases}$$

Es ist nicht schwer zu sehen, daß $\sum_{i=1}^n b_{ij} = 0$ sowie $\sum_{i=1}^n b_{ji} = 0$ für alle i gilt sowie $J(\mathfrak{G})^T = -J(\mathfrak{G})$. Hierbei ist $J(\mathfrak{G})^T := (b_{ji})_{ij}$. Wir machen jedoch im Folgenden keine Einschränkungen an $\mathfrak{G}$.

Definition 0.94 *Ein* ***Netzwerk über*** $\mathbb{R}$ *ist ein Qaudrupel $\langle\langle E, K\rangle, p, q, \gamma\rangle$, wo $\langle E, K\rangle$ ein gerichteter Graph, $p, q \in E$ und $\gamma : K \to \mathbb{R}$ eine Funktion mit $\gamma(k) \geq 0$ für alle $k \in K$. p heißt die* ***Quelle*** *und q die* ***Senke*** *des Netzwerks und γ die* ***Kapazität****.*

Analog wird ein *Netzwerk über* $\mathbb{N}_0$ defininiert. Die Idee hinter dieser Definition ist diese. In einem System von Kanälen (Leitungen, Straßen) hat jeder Weg seine charakteristische Kapazität (Leitfähigkeit). Wir wollen uns damit beschäftigen, wie man Flüsse in einem solchen System beschreiben kann und werden seine maximale Auslastung bestimmen. Dies ist bei Transportproblemen aber auch beim Auslegen von Schaltkreisen eine sehr wichtige Angelegenheit. Ein **Fluß** ist eine Funktion $f : K \to \mathbb{R}$ mit $f(k) \geq 0$ für alle $k \in K$. Gegeben f, definiere ∂f durch

$$(\partial f)(u) := \sum_{k^+ = u} f(k) - \sum_{k^- = u} f(k)$$

Die Funktion ∂f mißt in jedem Punkt die Differenz zwischen dem Einfluß und Ausfluß. Dies ist der sogenannte **Nettofluß**.

Definition 0.95 *Ein Fluß in einem Netzwerk $\langle E, K\rangle$ mit Quelle p, Senke q und Kapazität γ heißt* ***zulässig****, falls*

1. $0 \leq f(k) \leq \gamma(k)$ *für alle* $k \in K$.
2. $(\partial f)(u) = 0$ *für alle* $u \in E - \{p, q\}$.

Gegeben ein zulässiger Fluß können wir uns fragen, wie hoch der Gesamtdurchfluß ist. Dies ist gleich dem gesamten Fluß aus p, der Quelle, oder genau gleich dem gesamten Fluß in die Senke q. Denn es ist

$$0 = \sum_{x \in E} (\partial f)(x) = (\partial f)(p) + (\partial f)(q)$$

Daher ist also $(\partial f)(q) = -(\partial f)(p)$. Wir nennen $w(f) := -(\partial f)(p)$ den **Wert** des Flusses f. Die Frage, die sich stellt, ist nun, wie groß der Wert eines Flusses sein kann.

Definition 0.96 *Es sei ein Netzwerk gegeben aus $\langle E, K\rangle$, der Quelle p, der Senke q und der Kapazität γ. Es sei $E = X \cup Y$ mit $X \cap Y = \emptyset$, $p \in X$ und $q \in Y$. Das Paar $\langle X, Y\rangle$ heißt dann ein* ***Schnitt****. Die* ***Kapazität*** *des Schnittes, $c(X, Y)$, wird errechnet durch*

$$c(X, Y) := \sum_{k^- \in X, k^+ \in Y} \gamma(k)$$

Satz 0.97 *Es sei ein Netzwerk gegeben, f ein zulässiger Fluß und $\langle X, Y\rangle$ ein Schnitt dieses Netzwerkes. Dann gilt*

$$w(f) \leq c(X, Y)$$

Beweis. Für eine Partition $\langle A, B\rangle$ sei $S(A, B) := \{k \in K : k^- \in A, k^+ \in B\}$. Es gilt nun

$$w(f) = (\partial f)(q) = \sum_{u \in Y} (\partial f)(u)$$

Es ist ja $(\partial f)(u)$ die Differenz zwischen $\sum_{k^+ \in u} f(k)$ und $\sum_{k^- \in u} f(k)$. Wir können also in $(\partial f)(u)$ zwei Sorten Kanten entdecken: solche, deren beide Ecken in Y liegen, und solche, deren eine Ecke in X und deren andere Ecke in Y liegt. Der Beitrag einer Kante der ersten Sorte taucht in der obenstehenden Summe einmal positiv und einmal negativ auf, und so kann man die Beiträge dieser Kanten weglassen. Also ist

$$w(f) = \sum_{k \in S(X,Y)} f(k) - \sum_{k \in S(Y,X)} f(k) \leq \sum_{k \in S(X,Y)} f(k) \leq \sum_{k \in S(X,Y)} \gamma(k) = c(X, Y)$$

Dies zeigt die Behauptung. Q. E. D.

Ohne Beweis stellen wir folgenden Satz vor.

Satz 0.98 *Es sei N ein Netzwerk. Dann gilt*

$$min\{c(X,Y) : \langle X,Y\rangle \text{ Schnitt}\} = max\{w(f) : f \text{ zulässiger Fluß}\}$$

Dieser Satz gilt im Übrigen auch für Flüsse über $\mathbb{N}_0$. In diesem Fall existiert ein maximaler Fluß mit $f(k) \in \mathbb{N}_0$. Wir leiten daraus den Satz 0.89 her. Sei ein bipartiter Graph $\mathfrak{G} := \langle S+T, K\rangle$ gegeben. Seien p und q neue Elemente. Dann setzen wir $\mathfrak{G}^* := \langle S+T+\{p,q\}, K^*\rangle$, wobei $K^* := K \cup \{\langle p,u\rangle : u \in S\} \cup \{\langle v,q\rangle : v \in T\}$. Schließlich sei $\gamma(k) := 1$ für jede Kante. Dann ist $\mathfrak{G}^*$ mit p als Quelle und q als Senke und Kapazität γ ein Netzwerk über $\mathbb{N}_0$. Ein zulässiger Fluß in diesem Netzwerk ist dann immer eine Funktion $f : K^* \to \{0,1\}$. Da für eine Ecke $u \in S$ stets $(\partial f)(u) = 0$ ist, so gibt es höchstens ein $v \in T$ mit $\langle u,v\rangle \in K^*$ (und somit $\langle u,v\rangle \in K$), sodaß $f(\langle u,v\rangle) = 1$. Wir bekommen also ein Matching $M(f)$ für diesen Fluß. Sei umgekehrt ein Matching L gegeben. Setze $f_L(\langle u,v\rangle) := 1$ genau dann, wenn $uv \in L$ (es sei also $f_L(\langle u,v\rangle) := 0$ falls $uv \notin L$); $f_L(\langle p,u\rangle) := 1$ genau dann, wenn u gematcht ist und $f_L(\langle v,q\rangle) := 1$ genau dann, wenn v gematcht ist. Dies definiert einen zulässigen Fluß, wie man leicht sieht. Sein Wert ist genau $\sharp L$. Diese Zuordnung zwischen zulässigen Flüssen und Matchings ist bijektiv, und wir haben $\sharp L \leq \sharp L'$ genau dann, wenn $f_L(k) \leq f_{L'}(k)$ für alle $k \in K^*$ (genau dann, wenn $f_L(k) \leq f_{L'}(k)$ für alle $k \in K$). Es folgt, daß ein Matching genau dann maximal ist, wenn der zugeordnete Fluß ein maximaler zulässiger Fluß ist. Wir haben jetzt also

$$max\{w(f) : f \text{ Fluß in } \mathfrak{G}^*\} = max\{\sharp L : L \text{ Matching in } \mathfrak{G}\}$$

Um nun abzuleiten, daß die minimale Kapazität von Schnitten in $\mathfrak{G}^*$ gleich der minimalen Größe von Trägern von $\mathfrak{G}$ ist, müssen wir etwas genauer hinsehen. Sei dazu $A \subseteq S$. Wir setzen dann $\sigma(A) := \langle X(A), Y(A)\rangle$, wobei $X(A) := \{p\} \cup A \cup N(A)$ ist und $Y(A) := \{q\} \cup (S-A) \cup (T-N(A))$. Dies ist sicher ein Schnitt. Berechnen wir seine Kapazität. Die Kapazität des Schnitts ist die Anzahl der Kanten von $X(A)$ nach $Y(A)$. Man sieht sehr leicht, daß es genau $\sharp(S-A) + \sharp N(A)$ Kanten gibt. Nun definieren wir auch einen Träger, nämlich $\tau(A) := (S-A) \cup N(A)$. Daß dies ein Träger ist, sieht man so. Eine Kante in $\mathfrak{G}$ ist entweder (a) in $A \times N(A)$ oder (b) $(S-A) \times T$. In beiden Fällen ist sie mit einer Ecke aus $\tau(A)$ inzident. Dieser Träger hat genauso viele Elemente, wie die Kapazität von $\sigma(A)$ angibt.

Es ist nun so, daß nicht alle Schnitte von der Form $\sigma(A)$ sind und nicht alle Träger von der Form $\tau(A)$. Wir müssen also zeigen, daß wenigstens ein minimaler Schnitt bzw. Träger diese Form hat. Für Träger ist dies leicht zu sehen. Sei U ein minimaler Träger. Setze $A := S - U$. Dann ist $S \cap U = S - A$. Da U Träger, muß nun gelten: $U \cap T \supseteq N(A)$. Denn jede Kante, die mit einem Punkt aus A inzident ist, muß mit einem Punkt aus U inzident sein, und dieser kann nur aus $N(A)$ stammen. Sicher gibt es für jedes $u \in N(A)$ eine solche Kante, und daraus folgt $U \cap T \supseteq N(A)$. Daher gilt jetzt: $U \supseteq \tau(A)$. Falls also U minimal ist, gilt sogar $U = \tau(A)$. Es ist also sogar jeder minimale Träger von $\mathfrak{G}$ von der Form $\tau(A)$. Nun sei $\langle X^*, Y^*\rangle$ ein Schnitt von $\mathfrak{G}^*$ mit minimaler Kapazität. Dann setze $A := X^* \cap S$. Wir zeigen, daß $\sigma(A)$

die gleiche Kapazität hat wie $\langle X^*, Y^* \rangle$. Sind diese Schnitte nicht gleich, so existiert entweder (a) ein Punkt $y \in Y^* \cap T$, der auch in $N(A)$ ist oder (b) ein Punkt $x \in X^* \cap T$, der nicht in $N(A)$ ist. Wir zeigen zunächst, daß (b) nicht eintritt. Denn wenn $x \in (X^* \cap T) - N(A)$, so ist $\langle X^{**}, Y^{**} \rangle$ definiert durch $X^{**} := X^* - \{x\}$ und $Y^{**} := Y^* \cup \{x\}$ ein Schnitt mit geringerer Kapazität. Also $X^* \cap T \subseteq N(A)$. Sei also (a) der Fall. Dann sei $X^{**} := X^* \cup \{y\}$, $Y^{**} := Y^* - \{y\}$. Dann hat $\langle X^{**}, Y^{**} \rangle$ höchstens die Kapazität von $\langle X^*, Y^* \rangle$. Also haben, nach Voraussetzung, beide die gleiche Kapazität. Also existiert ein Schnitt $\langle X^*, Y^* \rangle$ minimaler Kapazität derart, daß Y^* disjunkt zu $N(A)$ ist. Da dann auch $X^* \cap T \subseteq N(A)$ gelten muß, ist dann $X^* \cap T = N(A)$, und so $\langle X^*, Y^* \rangle = \sigma(A)$ mit $A := X^* \cap S$. Dies zeigt nun, daß es minimale Schnitte der Form $\sigma(A)$ gibt. Daraus folgt jetzt

$$max\{w(f) : f \textit{ Fluß in } \mathfrak{G}^*\} = max\{\sharp L : L \textit{ Matching in } \mathfrak{G}\}$$

Wegen Satz 0.98 gilt

$$max\{w(f) : f \textit{ Fluß in } \mathfrak{G}^*\} = min\{c(\langle X, Y \rangle : \ \langle X, Y \rangle \textit{Schnitt von } \mathfrak{G}^*\}$$

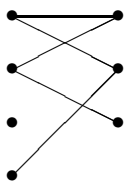
und damit

$$max\{\sharp L : L \textit{ Matching in } \mathfrak{G}\} = min\{T : T \textit{ Träger von } \mathfrak{G}\} \ .$$

und das ist die Aussage von Satz 0.89.

Übungen

Übung 51. Es sei folgender bipartiter Graph gegeben.



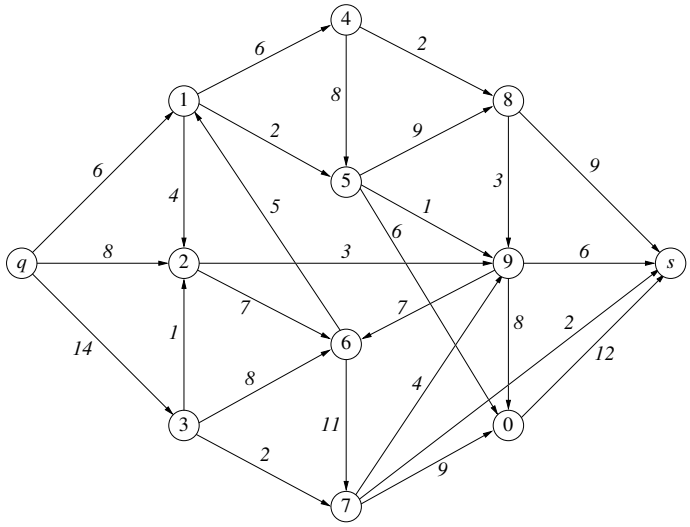
Bestimmen Sie das zugehörige Netzwerk $\mathfrak{G}^*$. Geben Sie einen Fluß maximalen Werts an sowie einen Schnitt minimaler Kapazität. Bestimmen Sie daraus ein maximales Matching und einen minimalen Träger.

Übung 52. Es sei $\mathfrak{G} = \langle E, K \rangle$ ein gerichteter Graph. Dann sei $u(\mathfrak{G}) := \langle E, \{uv : \langle u, v \rangle \in K\} \rangle$. $u(\mathfrak{G})$ ist der durch $\mathfrak{G}$ definierte ungerichtete Graph. Gegeben $\mathfrak{H}$, wie viele $\mathfrak{G}$ gibt es mit $u(\mathfrak{G}) = \mathfrak{H}$?

Übung 53. Zeigen Sie, daß es $\mathfrak{G}$ und $\mathfrak{H}$ gibt derart, daß $u(\mathfrak{G})$ und $u(\mathfrak{H})$ isomorph sind, nicht aber $\mathfrak{G}$ und $\mathfrak{H}$.

Übung 54. Es sei $\mathfrak{G}$ ein Netzwerk über $\mathbb{R}$, mit Quelle p Senke q und Kapazität γ. Zeigen Sie: ist f und g ein zulässiger Fluß, so auch $h := \lambda f + (1-\lambda)g$, wobei $0 \leq \lambda \leq 1$. Man berechne den Wert des Flusses. Zeigen Sie, daß h maximal ist, wenn es sowohl f als auch g sind.

Übung 55. Bestimme einen maximalen Fluß von q nach s in dem folgenden gerichteten Graphen. Die Zahlen an den Kanten bezeichnen die Kapazität.



Hinweis. Versuchen Sie zunächst einmal, einen niedrigen Wert für die Kapazität eines Schnittes zu erreichen. Falls Sie glauben, einen minimalen Wert erreicht zu haben, versuchen Sie, einen zulässigen Fluß mit diesem Wert zu finden.

Teil 12. Codierung I. Datenkompression.

Das Material zu den folgenden drei Teilen stammt aus R.–H. Schulz: *Codierungstheorie*, Vieweg Verlag, 1991. Vordergründig geht es bei der Codierung darum, eine Nachricht (**Quelltext**) in einer gewissen Form umzuschreiben (also nicht, ihn in eine andere Sprache zu übersetzen); dabei erhält man den **Zieltext**. Dabei kann dies aus mehreren Gründen geschehen; einerseits, weil der Quelltext in seiner gegebenen Form nicht aufgenommen werden kann (zum Beispiel, weil wie im Computer das gewöhnliche Alphabet nicht vorhanden ist), weil der Quelltext gekürzt werden könnte (man sagt, er sei *redundant*), weil bei der Übertragung Fehler auftreten können, und schließlich, weil ein Fremder den Text lesen könnte und man das nicht immer will. Je nach Umstand und je nach dem, was man vermeiden möchte, sind also ganz verschiedene Techniken der Codierung gefragt.

Definition 0.99 *Ein* ***Code*** *mit* ***Quellalphabet*** A *und* ***Zielalphabet*** B *ist ein Paar* $\langle \varphi, \psi \rangle$ *von berechenbaren Funktionen mit* $\varphi : A^* \to B^*$ *und* $\psi : B^* \to A^* \cup \{\sharp\}$ *derart, daß (1)* $\psi \circ \varphi(\vec{x}) = \vec{x}$ *für alle* $\vec{x} \in A^*$*, (2)*

$\psi(\vec{y}) = \sharp$ für alle $\vec{y}$, welche nicht von der Form $\varphi(\vec{x})$ sind. φ heißt die ***Verschlüsselungsvorschrift*** *und ψ die* ***Entschlüsselungsvorschrift****. $\vec{x} \in B^*$ heißt* ***Codewort****, falls ein $\vec{y} \in A^*$ existiert mit $\varphi(\vec{y}) = \vec{x}$.*

Haben wir einen Code $\langle \varphi, \psi \rangle$, so sagen wir, daß wir Zeichenreihen über A durch Zeichenreihen über B codieren. Es ist klar, daß φ injektiv und ψ surjektiv (auf B^*) sein muß. Die Definition verlangt nicht, daß das Codieren oder Decodieren einfach sein muß. In der Tat sind gerade die Methoden zur Datenkompression oder auch die fehlerkorrigierenden Codes nicht ganz einfach zu handhaben (wenn auch algorithmisch nicht besonders schwierig). Da es jedoch nicht einfach ist zu sagen, was eine leichte oder eine schwere Vorschrift ist, haben wir dies aus dem Spiel gelassen. Die einfachste Rechenvorschrift ist zweifellos das zeichenweise Übersetzen. Wie schon in Teil 4 angedeutet, kann man Alphabete ineinander übersetzen, wenn sie nur mindestens zwei Zeichen enthalten. Seien nämlich A, B endliche Alphabete und $v : A \to B^*$. Dann existiert genau ein Homomorphismus $\overline{v} : A^* \to B^*$. Wie kann man nun $\overline{v}$ umkehren?

Satz 0.100 *Es sei $v : A \to B^*$. Es gebe keine zwei Zeichen $a, a' \in A$ mit $a \neq a'$ derart, daß $v(a)$ ein Präfix von $v(a')$ ist. Dann existiert eine berechenbare Umkehrabbildung $\psi : B^* \to A^* \cup \{\sharp\}$ von $\overline{v}$.*

Beweis. $\overline{v}$ ist injektiv. Denn sei $\vec{x} = x_1 x_2 \ldots x_m \in A^*$ und $\vec{y} = y_1 y_2 \ldots y_n \in A^*$ sowie $\overline{v}(\vec{x}) = \overline{v}(\vec{y})$. Dann ist $v(x_1)$ ein Präfix von $\overline{v}(\vec{y})$ und so entweder $v(x_1)$ Präfix von $v(y_1)$ oder $v(y_1)$ Präfix von $v(x_1)$. Daher $x_1 = y_1$ und so $\overline{v}(x_2 x_3 \ldots x_m) = \overline{v}(y_2 y_3 \ldots y_n)$. Wiederholt man diese Argument, bekommt man $m = n$ und $\vec{x} = \vec{y}$. Wie sieht nun die Rückübersetzung aus? Das Verfahren ist denkbar einfach. Wir betrachten $\vec{y} \in B^*$. Sei $\vec{y} = y_1 y_2 \ldots y_n$. Wir betrachten dasjenige i mit $y_1 y_2 \ldots y_i = v(a)$ für ein $a \in A$ — sofern dieses existiert. Existiert es nicht, sei $\psi(\vec{y}) := \sharp$. Existiert es, sei $x_1 := a$, und es sei $\vec{y}^1 := y_{i+1} y_{i+2} \ldots y_n$. Fahre mit $\vec{y}^1$ fort und berechne so x_2, $\vec{y}^2$ und so weiter. Das Verfahren endet entweder damit, daß alle Zeichen gelesen sind und eine Zeichenkette $x_1 x_2 \ldots x_k$ konstruiert ist, oder daß $\sharp$ ausgegeben wird. Im ersten Fall sieht man sofort, daß $\overline{v}(\vec{x}) = \vec{y}$. Im zweiten Falle existiert keine Zeichenkette in A^*, deren Bild $\vec{y}$ ist. Q. E. D.

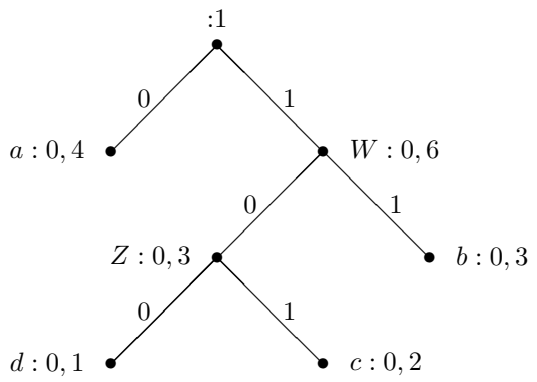
Wir sagen, eine Abbildung $v : A \to B^*$ habe die **Präfixeigenschaft**, falls für alle $a, a' \in A$ mit $a \neq a'$ gilt: $v(a)$ ist nicht Präfix von $v(a')$. Die billigste Variante, die Präfixeigenschaft sicherzustellen, ist die Codierung durch gleichlange Blöcke im Zielalphabet. Ein Beispiel ist der ASCII–Code. Das Ausgangsalphabet besteht aus 128 Zeichen, das Zielalphabet aus nur zwei, 0 und 1. Jedem Zeichen aus A ordnen wir eine Folge über $\{0, 1\}$ der Länge 7 zu. Diese Zuordnung ist bijektiv. (In Wirklichkeit besteht der Code aus 8 Zeichen, aber nur 7 werden gebraucht; das achte Zeichen ist das sogenannte *Prüfbit*. Damit werden wir uns noch befassen.)

Diese Verfahren ist relativ einfach zu handhaben, hat aber einen Nachteil: die übersetzten Texte sind oft länger als nötig. Dies ist relevant immer dann, wenn man Texte abspeichern möchte und Platz knapp ist. Um das genauer darzustellen, überlegen wir uns, daß die Zeichen unseres Alphabets nicht mit

der gleichen Häufigkeit auftreten. Zum Beispiel ist der Buchstabe ‘e’ der bei weitem häufigste Buchstabe. Es ist also plausibel, daß ein Code, der ‘e’ ein relative kurzes Wort über B zuweist, im Durchschnitt kürzere Texte erzeugt als ein anderer Code, der dies nicht tut. Wir nehmen nun an, wir hätten für jedes Zeichen aus A die Wahrscheinlichkeit $p(a)$ seiner Auftretens in einem beliebigen Textes ermittelt. Die beste Codierung im Falle, daß $B = \{0, 1\}$, ist die Codierung von *Huffman*. Man geht so vor. Seien a_1 und a_2 diejenigen Buchstaben mit der kleinsten Wahrscheinlichkeit. Ist $A = \{a_1, a_2\}$, so setze $v(a_1) := 0$ und $v(a_2) := 1$. Ansonsten sei $v(a_1) := \vec{x}0$ und $v(a_2) := \vec{x}1$ für ein noch zu bestimmendes $\vec{x}$. Ersetze A durch $A^1 := A - \{a_1, a_2\} \cup \{Z\}$, wobei Z ein neues Zeichen ist. Ferner sei $p^1(b) := p(b)$, falls $b \in A - \{a_1, a_2\}$ und $p^1(Z) := p(a_1) + p(a_2)$. Verfahre nun mit A^1 und p^1 wie mit A und p. Dies ergibt eine Vorschrift $v^1 : A^1 \to \{0, 1\}^*$. Setze $\vec{x} := v^1(Z)$.

Ein Beispiel. Es sei $A = \{a, b, c, d\}$ und $p(a) = 0,4$, $p(b) = 0,3$, $p(c) = 0,2$ und $p(d) = 0,1$.

a	b	c	d
$0,4$	$0,3$	$0,2$	$0,1$



Im ersten Schritt finden wir $v(d) = \vec{x}0$ und $v(c) = \vec{x}1$. $A^1 := \{a, b, Z\}$ mit $p^1(Z) = 0,3$. Nun sind c und Z die Zeichen mit geringster Auftretenswahrscheinlichkeit. Also ist $v^1(Z) = \vec{y}0$ und $v^1(b) = \vec{y}1$. Nun sei $A^2 := \{a, W\}$, $p^2(W) = 0,6$. Setze nun $v^2(a) := 0$, $v^2(W) := 1$. Es ist dann $v^1(Z) = v^2(W)0 = 10$, $v^1(b) = v^2(W)1 = 11$ und schließlich $v(c) = v^1(Z)1 = 101$, $v^1(Z)0 = 100$.

$$\begin{array}{lcl} a & \to & 0 \\ b & \to & 11 \\ c & \to & 101 \\ d & \to & 100 \end{array}$$

Es sollte klar sein, daß dieses Verfahren nicht eindeutig ist. Oft hat man im Verlaufe der Berechnung eine Wahl, einerseits in der Zuweisung von 0 und 1 und wenn zwei gleiche Wahrscheinlichkeiten auftreten. Der Algorithums zur Erstellung eines Huffmann–Codes ist also greedy: die in jedem Schritt günstigste

Lösung sichert das optimale Ergebnis. Wir teilen ohne Beweis mit, daß die Huffman–Codierung optimal in dem Sinne ist, daß die Zieltexte im Durchschnitt am kürzesten sind. Dies gilt allerdings nur, wenn die Auftretenswahrscheinlichkeit der Buchstaben im Quelltext wie angegeben ist und die Quelle, wie man sagt, kein Gedächtnis hat. Die Huffman–Codierung muß also nicht die beste Codierung überhaupt sein (falls es so etwas gibt). Eine Möglichkeit der Verbesserung ist die sogenannte *Blockcodierung*. Wir fügen zu A ein Symbol $\diamondsuit$ hinzu. Es sei ferner n eine natürliche Zahl, mindestens 1. Ein Quelltext wird von links nach rechts in Blöcke der Länge n geteilt. Geht dies nicht ganz auf (das heißt, seine Länge ist kein Vielfaches von n), so füllen wir den Quelltext am Ende mit $\diamondsuit$ auf. (Nur dafür müssen wir $\diamondsuit$ einführen. Da in der normalen Sprache ein Symbol existiert, das man ohne Schaden hinzufügen kann — nämlich das Leerzeichen —, entfällt die Notwendigkeit eines gesonderten Zeichens $\diamondsuit$.) Nun übersetzen wir anstelle von Buchstaben aus A, Blöcke über $A \cup \{\diamondsuit\}$ der Länge n. Hat A k Zeichen, so haben wir insgesamt $(k+1)^n$ Blöcke zu übersetzen. Der Witz ist nun, daß wir dies wieder mit Hilfe der Huffman–Codierung tun können. Warum sparen wir dabei? Es stellt sich heraus, daß die Häufigkeit des Auftretens eines Einzelzeichens auch von dem Kontext abhängt, in dem es auftritt. Zum Beispiel ist die Wahrscheinlichkeit, daß nach 'e' erneut 'e' auftritt, sehr klein, obwohl 'e' ja sehr häufig ist. Wir sprechen in diesem Zusammenhang davon, die Quelle *habe ein Gedächtnis*.

Betrachten wir erneut unser Alphabet $A = \{a, b, c, d\}$. Sei p wie folgt

aa	ab	ac	ad	ba	bb	bc	bd
$0,16$	$0,12$	$0,08$	$0,04$	$0,12$	$0,09$	$0,06$	$0,03$
ca	cb	cc	cd	da	db	dc	dd
$0,08$	$0,06$	$0,04$	$0,02$	$0,04$	$0,03$	$0,02$	$0,01$

Wir ignorieren zunächst das zusätzliche Symbol. Man findet folgende Codierung w

aa	ab	ac	ad	ba	bb	bc	bd
100	111	1010	0111	000	010	0010	11010
ca	cb	cc	cd	da	db	dc	dd
1011	0011	11001	01101	11000	01100	110110	110111

Wieso hat man nun damit etwas erreicht? Wir definieren dazu die sogenannte **mittlere Wortlänge**. Diese sei

$$\overline{\ell}(v) := \sum_{a \in A} p(a) \cdot \ell(v(a))$$

wobei $\ell(v(a))$ die Länge der Folge $v(a)$ ist. Es gilt für den Blockcode

$$\begin{aligned} \overline{\ell}(w) = & \ \tfrac{1}{100} \cdot \{3 \cdot (16+12+12+9) + 4 \cdot (8+8+6+6+4) + \\ & \quad 5 \cdot (4+4+3+3+2) + 6 \cdot (2+1)\} \\ = & \ 3,73 \end{aligned}$$

Da wir aber Blöcke der Länge 2 haben, so ist die mittlere Länge bezogen auf $\{a, b, c, d\}$ genau die Hälfte, also $1,865$. Im Falle der Ausgangscodierung bekommen wir $\frac{1}{100} \cdot \{1 \cdot 40 + 2 \cdot 30 + 3 \cdot 20 + 3 \cdot 10\} = \frac{1}{100} \cdot 190 = 1,9$, also leicht schlechter als bei der Blockcodierung.

Nun wollen wir uns dem vernachlässigten Symbol $\diamondsuit$ zuwenden. Man überlege sich, daß von den neun Zweierblöcken, die man mit $\diamondsuit$ und dem alten Alphabet zusätzlich erhält, nur vier braucht, nämlich $a\diamondsuit$, $b\diamondsuit$, $c\diamondsuit$ und $d\diamondsuit$. Die anderen habe jeweils Wahrscheinlichkeit Null des Auftretens. Wie groß ist die Wahrscheinlichkeit, einen solchen Zweierblock anzutreffen? Da er nur am Ende auftritt, hängt dies von der Länge des Textes ab. Falls die übertragenen Texte nur hinreichend groß sind (zum Beispiel dreihundert Zeichen), so sinkt die Summe der Wahrscheinlichkeit für alle vier Blöcke unter die kleinste Wahrscheinlichkeit, in diesem Falle also $0,01$. Man kann sich dann überlegen, daß der Huffman–Code sich nur für dd ändert. Insgesamt sieht eine mögliche Variante dann so aus.

dd	$a\diamondsuit$	$b\diamondsuit$	$c\diamondsuit$	$d\diamondsuit$
1101111	110111000	110111001	110111010	110111011

Für natürliche Sprache ist die Blockcodierung nicht die beste Form der Codierung. Es stellt sich heraus, daß man die Blöcke in der Länge variabel machen muß. Die 50 häufigsten Worte machen immerhin 50 % eines durchschnittlichen Textes aus, sodaß es sich offensichtlich lohnt, für diese jeweils einen Block zu reservieren. Ansonsten tut man gut daran, Silben als Blöcke zu nehmen. Wir wollen das jedoch nicht weiter verfolgen. Eine ganz andere Form der Codierung muß man wählen, wenn die Quelltexte deutlich anderer Natur sind. Ein Beispiel sind die Pixel–Codierung von Buchstaben. Um Buchstaben zu drucken, werden sie in winzige Punkte zerlegt, die entweder schwarz oder weiß sind. Diese Punkte heißen Pixel. Ein Buchstabe (als materielles Zeichen) ist also eine Bitsequenz, welche die Farbe des jeweiligen Pixels angibt. Es stellt sich heraus, daß die Farbe des folgenden Pixels in der Sequenz mit hoher Wahrscheinlichkeit der des vorangegangenen Pixels gleich ist. Daher kann man Pixelfolgen am zum Beispiel dadurch codieren, daß man sie als Zahlenfolgen $n_1, n_2, \ldots, n_k$ codiert, wobei n_1 die Anzahl der ersten weißen Pixel, n_2 die Anzahl der folgenden schwarzen Pixel, n_3 die Anzahl der darauffolgenden weißen Pixel und so weiter. Wir verlangen noch, daß alle $n_i > 0$ für $i > 1$. Es gibt natürlich viele andere Möglichkeiten. Es ist aber klar, daß man bei der Datenkompression immer damit berücksichtigen muß, um welchen Typ Daten es sich handelt.

Übungen

Übung 56. Es sei $\varphi : A^* \to B^*$ eine surjektive berechenbare Funktion. Konstruieren sie eine Berechnungsvorschrift für φ^{-1}. Damit ist also $\langle \varphi, \varphi^{-1} \rangle$ ein Code.

Übung 57. Zeigen Sie, daß der Huffman–Code die Präfixeigenschaft hat.

Übung 58. Es sei $\langle \varphi, \psi \rangle$ ein Code mit $\varphi : A^* \to B^*$, $\langle \varphi', \psi' \rangle$ ein Code mit

$\varphi : B^* \to C^*$. Konstruieren Sie eine Berechnungsvorschrift $\zeta : C^* \to A^* \cup \{\sharp\}$ derart, daß das Paar $\langle \varphi' \circ \varphi, \zeta \rangle$ ein Code ist. *Anmerkung.* Dieser Sachverhalt begründet unter anderem die gängige Praxis, mehrere Datenkompressionsverfahren zu kaskadieren. In UNIX kann man zum Beispiel erst mit `tar` ein Archiv aus vielen Dateien kreieren und es dann mit `compress` oder `zip` komprimieren. Man überlege sich anhand der Übungsaufgabe, warum es sinnvoll ist, daß die Datenkompressionsprogramme an den Dateinamen eine Erweiterung (`.tar` oder `.Z` oder `.gz`) anhängen.

Übung 59. Es sei $\sharp A > 1$. Der Huffman–Code hat folgende Eigenschaft. Zu jedem Wort $\vec{x} \in B^*$ existiert ein $a \in A$ und ein Suffix $\vec{y}$ von $\varphi(a)$ derart, daß $\vec{x}\vec{y}$ ein Codewort ist.

Übung 60. Man konstruiere einen Huffman–Code für folgende Wahrscheinlichkeiten.

A	B	C	D	E	F	G	H
$0,08$	$0,16$	$0,08$	$0,06$	$0,10$	$0,07$	$0,07$	$0,05$
I	J	K	L	M	N	O	P
$0,13$	$0,03$	$0,01$	$0,02$	$0,07$	$0,03$	$0,03$	$0,01$

Teil 13. Codierung II. Sicherheit.

Codierung kann auch einem anderen Zweck dienen, nämlich, die korrekte Übertragung von Daten zu gewährleisten. Man überlege sich, daß es ziemlich leicht vorkommen kann, daß die ursprüngliche Nachricht nicht korrekt übermittelt wird. Bei der Übertragung durch eine Leitung oder die Luft kann es zu atmosphärischen Störungen kommen; wenn wir einen Text niederschreiben oder in einen Rechner eintippen, machen wir gewisse Fehler. Das kann empfindliche Konsequenzen haben, und man sucht deshalb, dies zu vermeiden. Dies geschieht dadurch, daß der Code nunmehr zwei Teile enthält, einen, der zur Erstellung des Quelltextes dient, einen anderen, der die korrekte Übertragung sichert. Dabei bieten sich grundsätzlich zwei Lösungen an. (1.) Man ist daran interessiert, auftretende Fehler so oft wie möglich selbständig reparieren zu können oder (2.) man ist lediglich an der Identifikation von Fehlern interessiert. Das zweite Verfahren bietet sich immer dann an, wenn man interaktiv arbeitet, also im Notfall den Zieltext nochmals besorgen kann. Das erste bietet sich an, wenn man mit dem einmal gesendeten Zieltext auskommen muß. Grundsätzlich ist klar, daß man nicht alle Fehler ausschalten kann. Ein Text kann mit gewisser Wahrscheinlichkeit so verunstaltet werden, daß eine Rekonstruktion ohne Kenntnis des Quelltextes unmöglich ist. Daher reduzieren wir das Problem wie folgt. Wir betrachten Blockcodierungen mit fester Blocklänge n. Ferner habe jedes $\varphi(\vec{x})$ für einen Block $\vec{x}$ die gleiche Länge. Jedem Block $\vec{x}$ wird ein zunächst ein Codewort $\varphi(\vec{x})$ zugeordnet und anschließend ein sogenanntes **Kontrollwort** $\gamma(\vec{x})$. Das vollständige Codewort ist dann $\varphi(\vec{x})\gamma(\vec{x})$. Wir wollen $\gamma(\vec{x})$ so gestalten, daß

im Falle (1.) lediglich ein Fehler repariert werden kann, im Falle (2.) lediglich ein Fehler erkannt wird.

Im Folgenden wird es sich als nützlich erweisen, wenn wir den Buchstaben des Quellalphabets A sowie des Zielalphabets B jeweils natürliche Zahlen zuordnen. Dann dürfen wir sogar ohne Beschränkung der Allgemeinheit annehmen, daß $A, B \subseteq \mathbb{N}_0$ ist. Sehr oft macht es zum Beispiel so, daß A die Zahl 1, B die Zahl 2, C die Zahl 3 erhält — und so fort.

Wir wollen uns zunächst mit dem Problem der Fehleridentifikation befassen. Das simpelste Verfahren ist das Verfahren des **Kontrollbits**. Wir betrachten eine Codierung über $\{0, 1\}$. Es bezeichne

$$Q(\vec{y}) := y_1 + y_2 + \ldots y_n \pmod 2$$

die sogenannte **Quersumme**. Zum Beispiel sei $\gamma(\vec{x})$ so gewählt, daß

$$Q(\varphi(\vec{x})\gamma(\vec{x})) = Q(\varphi(\vec{x})) + Q(\gamma(\vec{x})) = 0$$

Genau dies wird beim ASCII–Code gemacht. Lautet zum Beispiel der Code des Zeichens L 0011001, so wird nun noch 1 angehängt. Damit erhält man den endgültigen Code 00110011 für L. Falls nun bei der Übertragung ein einzelner Fehler unterläuft (also ein Bit 'umklappt'), so wird dies sofort diagnostiziert, indem wir die Quersumme des empfangenen Blocks nehmen. Sei nämlich $\vec{y}$ ein Block der Länge 8; und sei $\vec{y}$ das Resultat aus einem Codewort $\vec{x}$ von höchstens einem Umklappen eines Bits. Dann ist $d(\vec{y}, \vec{x}) \leq 1$, also gilt $Q(\vec{y}) = Q(\vec{x})$ genau dann, wenn auch $\vec{y} = \vec{x}$ ist. Das Kontrollbit erlaubt also, einen Einzelfehler zu diagnostizieren. Es ist klar, daß wir nicht in der Lage sind, den Fehler auch zu reparieren. Falls wir dies wünschen, muß das Kontrollwort wesentlich länger sein Anschaulich gesprochen muß ja in dem Kontrollwort auch Information darüber enthalten sein, wo der Fehler aufgetaucht ist. Daher muß das Kontrollwort mindestens die Länge 3 haben, wenn das Gesamtwort die Länge 8 hat. Man beachte, daß wir ja auch Fehler im Kontrollwort einkalkulieren müssen!

Die Methode des Kontrollbits läßt sich verallgemeinern. Wir nehmen ein $v : A \to B$ derart, daß $v(a)$ jeweils ein Block der Länge κ ist. Sei $B = \{1, 2, \ldots, m\}$. Sei $\vec{x} = x_1 x_2 \ldots x_r$ eine beliebige Folge über B^*. Sei

$$Q(\vec{x}) := x_1 + x_2 + \ldots + x_r \pmod m$$

die Quersumme modulo m. Der Code, welcher durch $w(a) := v(a)u$, wo $u = m - Q(v(a))$, definiert ist, kann genau einen einfachen Tippfehler erkennen. Denn wird $\vec{y}$ gelesen, so bilde man $Q(\vec{y})$. Ist $\vec{y}$ in höchstens einem Symbol von einem Codewort verschieden, so ist $\vec{y}$ genau dann ein Codewort, wenn $Q(\vec{y}) = 0$.

Wenden wir uns der Möglichkeit zu, daß es auch noch andere als die einfachen Fehler gibt. Anstatt nun auf Doppelfehler überzugehen, kann man sich die Art der Fehler etwas genauer ansehen. Dazu eine Statistik.

Fehlertyp	Beschreibung	rel. Häufigkeit (in %)
Verwechslung (Einfachfehler)	$a \mapsto b$	79,0
Nachbartransposition	$ab \mapsto ba$	10,2
Sprungtransposition	$acb \mapsto bca$	0,8
Zwillingsfehler	$aa \mapsto bb$	0,6
übrige		9,4

Nach Möglichkeit wollen wir einen Code konstruieren, der Einzelfehler und Nachbartranspositionen erkennt. Eine Möglichkeit bietet der ISBN–Code (International Standard Book Number). Ein typisches ISBN Codewort sieht wie folgt aus 3-540-05303-4. Wichtig für uns ist die letzte Ziffer; sie ist die Prüfziffer. Sie ist eine Ziffer oder aber X — wir werden sehen, warum. Wir wollen der Einfachheit halber annehmen, es handelt sich um die identische Codierung, das heißt, wir haben es bei den ersten neun Ziffern gar nicht mit einer echten Codierung zu tun. Gegeben eine neunstellige Zahl $a_1a_2\ldots a_9$, definieren wir nun

$$b_{10} := \sum_{i=1}^{9} i \cdot a_i \pmod{11}$$

Zwei Dinge sind bemerkenswert. Zum einen die Tatsache, daß wir eine gewichtete Summe bilden und zum anderen, daß wir modulo 11 rechnen. Deswegen benötigen wir im übrigen auch das X. Denn wenn $b_{10} = 10$, so sei $a_{10} := X$, ansonsten aber $a_{10} := b_{10}$. Der Witz ist nun folgender. Dieser Code kann nicht nur einfache Tippfehler erkennen, sondern auch sämtliche Transpositions– und Sprungtranspositionsfehler! Um das zu sehen, sei $\vec{x} = x_1x_2\ldots x_{10}$ gegeben. (Der Einfachheit wegen sei X gleich 10 gesetzt.) Wir nehmen an, $\vec{x}$ sei durch einen Einfachfehler aus $\vec{a} := a_1a_2\ldots a_{10}$ entstanden. Sei etwa $a_j \neq x_j$. Dann berechnen wir

$$\xi(\vec{x}) := (\sum_{i=1}^{9} i \cdot x_i) - x_{10} \pmod{11}$$

Da $10 \equiv -1 \pmod{11}$, so ist

$$\xi(\vec{x}) = \sum_{i=1}^{10} i \cdot x_i$$

Im Übrigen ist auch $\xi(\vec{a}) = \sum_{i=1}^{10} i \cdot a_i$. Wir behaupten, daß $\xi(\vec{x}) \neq 0$. Dazu betrachten wir

$$\xi(\vec{a}) - \xi(\vec{x}) \equiv j \cdot (a_j - x_j) \pmod{11}$$

Hier kommt die Tatsache ins Spiel, daß 11 eine Primzahl ist. j hat ein multiplikatives Inverses, da $j \neq 0$ ist. Dies bedeutet, daß $j \cdot (a_j - x_j) \not\equiv 0 \pmod{11}$. Hätten wir also 10 statt 11 gewählt, wäre dies nicht möglich. Nun sei als zweites $\vec{x}$ durch einen Transpositionsfehler aus $\vec{a}$ entstanden, etwa sei $x_j = a_i$ und $x_i = a_j$ für gewisse $0 < i < j < 11$, ansonsten aber $a_k = x_k$. Dann ist

$$\xi(\vec{a}) - \xi(\vec{x}) = i \cdot a_i + j \cdot a_j - i \cdot a_j - j \cdot a_i = (i - j)(a_i - a_j)\ .$$

Es ist $(i-j)(a_i - a_j) \equiv 0$ genau dann, wenn $i = j$ (was ausgeschlossen ist) oder $a_i = a_j$ (in welchem Falle aber $\vec{x} = \vec{a}$). Wir können also Transpositionsfehler, Sprungtranspositionsfehler und mehr entdecken, insgesamt mehr als 90 % der Fehler.

Nun kommen wir zu der Fehlerkorrektur. Hier gibt es recht raffinierte Verfahren. Wir wollen uns aber mit ein paar Handgriffen zufriedengeben. Zunächst einmal wollen wir sehen, unter welchen Umständen eine Fehlerkorrektur möglich ist. Dazu konzentrieren wir uns der Einfachheit halber auf Bitfolgen. Wir erinnern daran, daß der **Hammingsabstand** $d(\vec{x}, \vec{y})$ zweier Bitfolgen gleicher Länge gleich der Anzahl der verschiedenen Bits in $\vec{x}$ und $\vec{y}$ ist, das heißt

$$d(\vec{x}, \vec{y}) := \sum_{x_i \neq y_i} 1 \ .$$

Es sei $\vec{x} \in \{0,1\}^n$. Dann ist $K_d(\vec{x}) := \{\vec{y} : d(\vec{y}, \vec{x}) \leq d\}$. Dies heißt die **Kugel** mit Radius d um $\vec{x}$. Ein Code heiße d–**korrigierend**, falls bei der Übertragung eines Codeworts bis zu d Fehler auftreten dürfen und dennoch das Codewort eindeutig identifiziert werden kann.

Satz 0.101 *Es sei $v : A \to \{0,1\}^n$ ein Code derart, daß zu je zwei Codeworten $v(a)$ und $v(b)$ mit $a \neq b$ gilt $K_d(v(a)) \cap K_d(v(b)) = \emptyset$. Dann ist v d–korrigierend.*

Beweis. Hat man $\vec{y}$ und ist $\vec{y}$ aus einem Codewort $v(a)$ entstanden durch höchsten d–fachem Umklappen eines Bits, so ist $d(\vec{y}, v(a)) \leq d$, mithin $\vec{y} \in K_d(v(a))$. Dann existiert nach Voraussetzung kein $b \neq a$ mit $d(\vec{y}, v(b)) \leq d$, also ist a eindeutig. Q. E. D.

Ein Code ist d–korrigierend, falls $d(v(a), v(b)) > 2d$ für alle $a, b \in A$ mit $a \neq b$. Ein Beispiel. Die Punkte $(0,0,0)$ und $(1,1,1)$ haben den Hamming–Abstand 3. Also können wir ein Informationsbit unterbringen, und können einen Fehler korrigieren. Wähle einfach $v : 0 \mapsto (0,0,0), 1 \mapsto (1,1,1)$. Die Ausbeute ist nicht gerade gut. Etwas besser ist folgender Code, der auf 7 Bits gerade 3 Kontrollbits enthält und einen Fehler korrigieren kann. Wir wollen ihn nicht im Detail studieren, sondern ohne Beweis angeben, wie er funktioniert. Es sei H folgende Matrix.

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

Das zu übertragende Wort sei (a, b, c, d). Dann seien x, y, z so gewählt, daß für den Vektor $\vec{v} := (x, y, a, z, b, c, d)$ gilt

$$H\vec{v} = \vec{0}$$

Um zu zeigen, daß dies tatsächlich ein 1–korrigierender Code ist, muß man einiges an algebraischen Hilfsmitteln bereitstellen. (Es zeigt sich also, daß höhere Mathematik am Ende doch ganz praktische Anwendungen haben kann.)

Dies sieht wesentlich besser aus. Jedoch sollte man bedenken, daß die Wahrscheinlichkeit, daß auf 7 Zeichen ein Fehler eintritt, höher ist, als daß auf 3 Zeichen ein Fehler eintritt. Bei 7 Zeichen geht man also schon eher das Risiko ein, daß man einen Doppelfehler hat (und ihn nicht erkennen kann). In Computern ist das Risiko von Doppelfehlern aber bei derart kurzen Worten vernachlässigbar klein.

Definition 0.102 *Die* ***Informationsrate*** *eines Codes mit Codeworten der Länge n über 2 ist definiert durch*

$$\log_2 \sharp A/n$$

Der erste Code hat eine Informationsrate von 1/3, der zweite von 4/7. Die Informationsrate ist von Belang, wenn man sich für den Aufwand bei der Datenübertragung interessiert. Der Kehrwert der Informationsrate mißt, um welchen Faktor der Zieltext länger wird wir der Quelltext. Falls man also die 3–Bit Codierung wählt, so ist der Zieltext immerhin dreimal so lang wie der Quelltext, bei der 7–Bit Codierung immerhin noch fast zweimal so lang!

Wir wollen zum Abschluß eine heuristische Überlegung anstellen, wie viele Codewörter wir unterbringen können, wenn die Blocklänge β gegeben ist und die Anzahl d der zu korrigierenden Fehler. Gewiß kann man immer mindestens ein Wort unterbringen! (In diesem Fall ist der zu übertragende Block stets bekannt, die Korrektur gelingt immer. Die Botschaft besteht also nur in der Länge des übertragenen Wortes. Dann ist die Maschinerie der Fehlerkorrektur natürlich höchst überflüssig.) Gegeben ein Codewort, muß es uns sagen, welches Symbol übertragen wurde, und an welcher Stelle Fehler aufgetreten sind. Es gibt

$$\sum_{j=0}^{d} \binom{\beta}{j}$$

viele Möglichkeiten, an einem Codewort bis zu d Fehler anzubringen. (Diese entsprechen gerade den Teilmengen der Menge $\{1, 2, \ldots, \beta\}$ der Mächtigkeit $\leq d$.) Wir haben insgesamt 2^β viele Blöcke zur Verfügung, also können wir höchstens

$$\frac{2^\beta}{\sum_{j=0}^{d} \binom{\beta}{j}}$$

Symbole kodieren. Diese Zahl ist in der Regel zu hoch, gibt aber erst mal eine Abschätzung. Für $d = 1$ ergibt sich die sogenannte *Hamming–Volumenschranke*

$$\frac{2^\beta}{\beta + 1}$$

also für $\beta = 2, 3, 4, 5$ gerade 1, 2, 3, 5.

Übungen

Übung 61. Die Europäische Artikelnummer (EAN) besteht aus dreizehn Dezimalziffern, wobei die letzte eine Prüfziffer ist. Sie wird wie folgt berechnet

$$a_{13} := -(1 \cdot a_1 + 3 \cdot a_2 + 1 \cdot a_3 + 3 \cdot a_4 + \ldots + 1 \cdot a_{11} + 3 \cdot a_{12}) \pmod{10}$$

Man überlege, ob der EAN–Code in der Lage ist, Einfachfehler und Transpositionsfehler zu erkennen.

Übung 62. Kann der ISBN–Code Zwillingsfehler erkennen? Wenn nein, welche genau nicht?

Übung 63. Man wähle n Stück Permutation π_n auf der Menge $\{0, 1, 2, \ldots, 9\}$. Dann sei a_n so bestimmt, daß eine Kontrollgleichung gilt für ein gewisses c.

$$c = \sum_{j=1}^{n} \pi_j(a_j) \pmod{10}$$

Zum Beispiel ist der Code der deutschen Postgironummern wie folgt.

$$\begin{array}{ccccccl} \pi_1 & = & \pi_4 & = & \pi_7 & = & (0)(124875)(36)(9) \\ \pi_2 & = & \pi_5 & = & \pi_8 & = & (026387514)(9) \\ \pi_3 & = & \pi_6 & = & \pi_9 & = & (0316)(29857) \end{array}$$

Schließlich sei $\pi_{10} = (0)(19)(28)(37)(46)(5)$. Zeigen Sie, daß dieser Code auf jeden Fall Einzelfehler erkennt. Wie steht es mit Nachbartranspositionen? (Alternative: Zwillingsfehler.) *Hinweis.* Da die Permutationen relativ willkürlich sind, kann man sich nur mit jeder Nachbartransposition einzeln befassen. Das kann ein bißchen langwierig werden, ist aber keinesfalls schwer.

Übung 64. Geben Sie d–korrigierende Codes an für jedes d und berechnen Sie deren Informationsrate.

Übung 65. Zeigen Sie, daß der folgende Code 1–korrigierend ist.

$$00 \mapsto \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad 01 \mapsto \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad 10 \mapsto \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \qquad 11 \mapsto \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Für Extrapunkte zeige man, daß es keinen 1–korrigierenden Code mit Blocklänge 5 gibt, der mehr als vier Codeworte hat.

Teil 14. Codierung III. Kryptographie.

Ein mit der Codierung häufig assoziierte Technik ist die *Kryptographie*. Hier geht es darum, eine Botschaft so zu übermitteln, daß sie von Dritten nicht

verstanden werden kann, die sie zufällig (oder weniger zufällig) zu lesen bekommen. Wir unterscheiden zwei grundlegend verschiedene Methoden. Die eine ist diejenige, bei der sowohl Sender als auch Empfänger in Besitz des Codes sind. Wir wollen diese *reversible* oder *symmetrische Geheimcodes* nennen. Die andere ist diejenige, bei der der Sender zwar verschlüsseln kann aber nicht entschlüsseln. Diese nennen wir *irreversible Geheimcodes*. Ein Code besteht, wie wir gesehen haben, aus einem Verschlüsselungsverfahren und einem Entschlüsselungsverfahren. Normalerweise ist es erwünscht, beide zu kennen. Die sogenannten *Public–Key–Systeme* sind aber so gedacht, daß jeder Teilnehmer den Verschlüsselungscode öffentlich macht, damit ihm jeder andere Teilnehmer eine Nachricht zukommen lassen kann, ohne daß dritte (auch nicht andere Teilnehmer) diese lesen können. Die Anforderungen an *Public–Key–Systeme* sind also hoch: nicht nur soll die Botschaft ohne Kenntnis des Codes nicht lesbar sein, sie soll auch *mit* Kenntnis des Verschlüsselungsverfahrens unlesbar sein! Dies bedeutet nichts anderes, als daß die Berechnung des Entschlüsselungsverfahrens aus dem Verschlüsselungsverfahren unmöglich gemacht wird. Da die Verschlüsselung blockweise geschieht, ist das Wort *unmöglich* allerdings unangebracht (siehe dazu auch die Übung 56). Man kann ja einfach alle Blöcke hintereinander verschlüsseln, und bekommt so eine Tabelle, in der man einfach nachschauen kann. Der Witz an den irreversiblen Codes ist also nicht, daß das Entschlüsseln wirklich unmöglich ist, sondern nur, daß der Aufwand dafür unvertretbar hoch ist (mehrere Jahre oder Jahrzehnte).

Betrachten wir zunächst die reversible Codierung. Die einfachste Methode (der sogenannte *Caesar–Code*) ist das Verschieben modulo 26 um eine feste Zahl. Wir ordnen den Buchstaben Zahlen zu in der folgenden Weise

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Unser Alphabet sei Ω, die Zuordnung $\zeta : \Omega \to \{0, 1, 2, 3, \ldots, 25\}$. Die Verschlüsselungsvorschrift ist dann $\varphi(a) := \zeta^{-1}(\zeta(a) + b)$, wobei wir modulo 26 rechnen. Dieser Code ist allerdings leicht zu knacken; man muß ja nur b erraten. Etwas schwieriger ist, wenn wir einfach auf der Grundlage einer beliebigen Bijektion $\pi : \Omega \to \Omega$ arbeiten. Es gibt so viele Bijektionen (26! Stück), daß das sture Durchprobieren nicht sinvoll ist. Allerdings ist man auch hier nicht chancenlos, wenn man ein längeres Stück Text hat. Dann errechne man einfach die Häufigkeit, mit der die Zeichen des Zieltextes auftreten. Diese müssen ja ungefähr den normalen Häufigkeiten entsprechen, mit denen das unverschlüsselte Gegenstück in Texten auftritt. Damit läßt sich das 'e' des Quelltextes und sein Code identifizieren — und sicher noch ein paar mehr Buchstaben. Ist man so weit gekommen, lassen sich die übrigen Buchstaben mit etwas Geschick erraten. Solche statistischen Überlegungen sind eine scharfe Waffe gegen Verschlüsselungsverfahren. (Wir wollen dies nicht weiter diskutieren; es sei nur angemerkt, daß man bei der Entschüsselung nur dann eine

Chance hat, wenn die Natur des Codes einigermaßen bekannt ist. Ohne solches Wissen (oder eine gute Vermutung) ist es aussichtslos.) Wir wollen das oben angegebene Verfahren nun gegen diesen statistischen Angriff wie folgt wappnen. Wir wählen eine nicht zu kurze Folge $\vec{b} = b_1 b_2 \dots b_p \in \Omega^p$. Dies kann in der Praxis einem sinnvollen Wort entsprechen, muß es aber nicht. Nun wird der Text wie folgt codiert

$$\varphi(x_1 x_2 \dots x_m) := y_1 y_2 \dots y_m$$

wobei $y_{jp+k} := \zeta^{-1}(\zeta(x_{jp+k}) + \zeta(b_k))$. Dies bedeutet, daß das Maß der Verschiebung von der Stelle abhängt, und von dem Wort $\vec{b}$ abhängt. Kennt der Empfänger diese Methode, so muß er nur $\vec{b}$ zusätzlich zu dem Zieltext kennen, und er kann den Quelltext berechnen. Dies Verfahren ist das Verfahren von *Vigenère*. Da ein fester Buchstabe je nach einer Stelle im Text auf einen anderen Zielbuchstaben geworfen wird, wird die Wahrscheinlichkeit des Quellbuchstaben maskiert. Wir bemerken, daß es reversible Verschüsselungsverfahren gibt (zum Beispiel das Verfahren von *Vernan*, die absolut sicher sind, sofern der (über eine Zufallsfolge ermittelte) Schlüssel geheim bleibt. Hier liegt die Schwachstelle dieser Verfahren, da sie mit einem variablen Schlüsselwort arbeiten, das ja erst einmal übertragen werden muß. Letzteres kann natürlich nur mit einem Code geschehen, der grundsätzlich nicht von dieser Art ist, also unsicher.

Damit beenden wir den Streifzug durch die reversiblen Verschlüsselungstechniken und wenden uns den irreversiblen zu. Wir stellen ein wenig bekanntes Verschlüsselungsverfahren vor. Es sei $A = \{0, 1, \dots, n\}$. Ferner seien Gewichte δ_j, $1 \leq p$, gegeben mit der Eigenschaft, daß $\delta_j > 0$ und $(n+1) \cdot \delta_j \leq \delta_{j+1}$. Gegeben ein Wort der Länge p, $\vec{a} = a_1 a_2 \dots a_p$, so sei $W(\vec{a})$ definiert durch

$$W(\vec{a}) := \sum_{j=1}^{p} \delta_j \cdot a_j$$

Ist $W(\vec{a})$ gegeben, so läßt sich sehr leicht $\vec{a}$ ermitteln. Wir zerlegen $P_p := W(\vec{a})$ in $P_p = b_p \cdot \delta_j + P_{p-1}$ derart, daß $P_p < \delta_p$. Ebenso zerlegen wir $P_{p-1} = b_{p-1}\delta_{p-1} + P_{p-2}$. Und so weiter. Falls im Verlaufe der Zerlegung ein $b_j > n$ oder $P_0 \neq 0$, so haben wir kein Codewort. Andernfalls haben wir die Entschlüsselung $\vec{b} = b_1 b_2 b_3 \dots b_p$. Wieso ist nun $\vec{b} = \vec{a}$? Dazu sei q der höchste Index $\leq p$ sodaß $a_q \neq b_q$. Wir nehmen an, daß $a_q > b_q$. Dann ist

$$0 = W(\vec{a}) - W(\vec{b}) = \sum_{j=1}^{q} (a_j - b_j)\delta_j$$

Man überlegt sich, daß $|a_j - b_j| \leq n$, daher ist die rechte Summe größer oder gleich

$$(a_q - b_q)\delta_q - \sum_{j=1}^{q-1} n\delta_j \geq \delta_q - \sum_{j=1}^{q-1} n\delta_j > \delta_1 > 0$$

Denn $n\delta_j \leq \delta_{j+1} - \delta_j$, sodaß

$$\sum_{j=1}^{q-1} n\delta_j \leq \sum_{j=1}^{q-1} \delta_{j+1} - \delta_j = \delta_q - \delta_1$$

Also haben wir ein Verschüsselungsverfahren gefunden. Der Nachteil ist, daß es leicht zu knacken ist. Um dies zu verhindern, bedienen wir uns eines Tricks. Wir wählen eine Primzahl r und eine Zahl u. Ferner sei $uv \equiv 1 \pmod{r}$. Einzige Bedingung an die Primzahl ist, daß kein Codewort $\geq r$ ist. Nun definieren wir als Verschlüsselungsverfahren $\vec{a} \mapsto V(\vec{a})$, wobei

$$V(\vec{a}) := \sum_{j=1}^{p} \gamma_j a_j$$

und $\gamma_j := u \cdot \delta_j \pmod{r}$. Für das Verschlüsseln müssen lediglich die Gewichte γ_j bekannt sein. Wenn man es gut macht, sind die Gewichte so bösartig verteilt, daß das Entschlüsseln sehr schwer fällt. Zum Entschlüsseln geht man so vor. Man erhälte die Zahl x. Man berechnet zunächst $v \cdot x \pmod{r}$ und zerlegt dann

$$v \cdot x = \sum_{j=1}^{p} \delta_j a_j \pmod{r}$$

Wie wir oben gesehen haben, ist dieses Problem sehr leicht. Daß wir damit korrekt entschlüsseln, belegt folgende Rechnung

$$\begin{aligned} v \cdot V(\vec{a}) &= v \textstyle\sum_{j=1}^{p} \gamma_j a_j \\ &= \textstyle\sum_{j=1}^{p} vu\delta_j a_j \\ &= \textstyle\sum_{j=1}^{p} \delta_j a_j \\ &= W(\vec{a}) \pmod{r} \end{aligned}$$

Ein Beispiel. Unser Alphabet sei $A = \{0, 1, 2\}$. Wir wollen Blöcke der Länge 5 codieren. Die Gewichte sind

δ_1	δ_2	δ_3	δ_4	δ_5
1	3	9	27	81

Offensichtlich ist $3\delta_j \leq \delta_{j+1}$, $1 \leq j \leq 4$. Die größte Zahl, die damit gebildet werden kann, ist $\sum_{j=1}^{5} 2\delta_j = 2(1 + 3 + 9 + 27 + 81) = 242$. Wir nehmen daher als Primzahl $r = 251$. Es gilt $69 \times 211 \equiv 1 \pmod{251}$. Wenn wir also die Gewichte mit 211 multiplizieren, erhalten wir die öffentlichen Gewichte

γ_1	γ_2	γ_3	γ_4	γ_5
211	131	142	175	23

Es werde zum Beispiel die Zahl 774 übermittelt. Dann ist $774 \equiv 21 \pmod{251}$. Wir berechnen $69 \cdot 21 = 1449 \equiv 194 \pmod{251}$. Es ist nun leicht zu ermitteln,

daß $194 = 2 \times 81 + 1 \times 27 + 1 \times 3 + 2 \times 1$, also ist die übermittelte Nachricht $(2, 1, 0, 1, 2)$. Zur Probe berechnen wir

$$2 \times 211 + 1 \times 131 + 0 \times 142 + 1 \times 175 + 2 \times 23 = 774$$

Dieses Verfahren wird dadurch sicher gemacht, daß man die Blocklänge groß wählt und die Primzahl ebenso. Wichtig ist, daß die offengelegten Gewichte gehörig durcheinandergewirbelt sind. Natürlich garantiert dies nicht, daß es nicht doch raffinierte Verfahren gibt, die das Problem der unbefugten Entschlüsselung in vertretbarer Zeit lösen. Man sollte jedenfalls auch hier im Auge behalten, daß man gegen solche Codes immer auch statistisch vorgehen kann, sodaß man auch hier etwas raffinierter vorgehen sollte. Man könnte das genannte Verfahren zum Beispiel mit der Methode von Vigenère kaskadieren. Das eben diskutierte Verfahren ist im Übrigen geknackt worden, sodaß man sich anderen Methoden zugewendet hat, so zum Beispiel dem RSA Algorithmus.