Total anti-symmetrische Quasigruppen

Dissertation
zur
Erlangung des Doktorgrades
der Naturwissenschaften
(Dr. rer. nat.)

dem
Fachbereich Mathematik und Informatik
der Philipps-Universität Marburg
vorgelegt von

H. Michael Damm

aus Marburg/Lahn

Marburg/Lahn 2004

Vom Fachbereich Mathematik und Informatik
der Philipps-Universität Marburg als Dissertation am 12. Mai 2004 angenommen.

Erstgutachter:	Prof. Dr. H. Peter Gumm
Zweitgutachter:	Prof. Dr. Ralph-Hardo Schulz

Tag der mündlichen Prüfung am 9. Juli 2004.

Inhaltsverzeichnis

Zusammenfassung

Bei der Untersuchung von Prüfziffersystemen über Quasigruppen stößt man auf die so genannten total anti-symmetrischen Quasigruppen. Bislang war ihre Existenz für alle Ordnungen $4k+2 \geq 10$ ungeklärt. Ecker und Poch vermuteten 1986, dass es keine total anti-symmetrischen Quasigruppen der Ordnung $4k+2$ gibt. In der vorliegenden Arbeit widerlegen wir diese Vermutung und entwickeln Konstruktionen für total anti-symmetrische Quasigruppen der Ordnung n für alle $n \neq 2, 6$. Per Computersuche weisen wir außerdem nach, dass Prüfziffersysteme über einer 2-Quasigruppe der Ordnung 10, ebenso wie Prüfziffersysteme über Gruppen der Ordnung 10, nicht alle (Sprung-)Zwillingsfehler oder Sprung-Transpositionen erkennen können. Als weiteres Ergebnis zeigen wir, dass die Klasse der total anti-symmetrischen Quasigruppen keine Varietät ist.

Kapitel 1

Einleitung

Die Informationstechnologie hat in unserem Alltag einen sehr hohen Stellenwert. Die Übermittlung von Daten erfolgt größtenteils elektronisch, allerdings werden z.B. durch eCommerce oder Homebanking immer mehr Zahlen von ungeübten Benutzern erfasst. Daher bekommt das frühzeitige Erkennen von Tippfehlern eine große Bedeutung. Abgesehen von falsch gelieferten Artikeln oder fehlerhaften Überweisungen kann ein Zahlendreher auch weiter reichende Konsequenzen haben. So wurde eine Akte mit brisanten Informationen über einen Prominenten statt an eine Anwaltskanzlei an einen Pizzabäcker gefaxt und damit der Öffentlichkeit zugänglich gemacht [67]. Der Prominente musste daraufhin seine politischen Ämter niederlegen. Zur Vermeidung solcher Probleme werden Zahlen mit Prüfziffern geschützt. Hierbei wird aus den vorhandenen Ziffern der zu schützenden Zahl eine weitere Ziffer berechnet - die Prüfziffer - welche am Ende angefügt wird. Bekannte Beispiele sind Kontonummern oder Bankleitzahlen, die EAN/UPC-Nummern von Artikeln oder die Seriennummern von Banknoten. Die meisten Prüfzifferverfahren beruhen auf der Berechnung mit einer Gruppe. Seltener wird eine Quasigruppe zur Berechnung benutzt, wie z.B. bei den Schweizer Einzahlungsscheinen. In [18] haben wir gezeigt, dass Prüfzifferverfahren über Gruppen der Ordnung 10 bestimmte Fehlerarten nicht erkennen können. Gegenstand dieser Arbeit ist daher ein allgemeinerer Ansatz mit total anti-symmetrischen Quasigruppen. Wir beschäftigen uns dabei ausführlich mit der Konstruktion dieser Quasigruppen und weisen deren Existenz nach. Weiterhin widerlegen wir eine Vermutung von Ecker und Poch, dass total anti-symmetrische Quasigruppen der Ordnung 4k+2 nicht existieren.

1.1 Fehlerstatistik

Bereits Ende der 60er Jahre untersuchte der holländische Mathematiker J. Verhoeff [66] die Art und die Häufigkeit von Tippfehlern bei der Eingabe von Zahlen. Er stellte dabei fest, dass Einzelfehler und Nachbarvertauschungen am häufigsten vorkommen. Mit etwas Abstand folgen (Sprung-)Zwillingsfehler und Sprung-Transpositionen (siehe Tabelle).

Fehlerart		Symbol	Verhoeff	Damm
1.	eine falsche Ziffer (Einzelfehler)	$x \to y$	79,0 %	62,3 %
2.	Nachbarvertauschung (Vertauschung einer Ziffer mit der nächsten)	$xy \to yx$	10,2 %	14,0 %
3.	Sprung-Transposition (Vertauschung einer Ziffer mit der übernächsten)	$xzy \to yzx$	0,8 %	0,9 %
4.	Zwillingsfehler	$xx \to yy$	0,6 %	1,3 %
5.	phonetische Fehler ($a = 2, ..., 9$)	$a0 \leftrightarrow 1a$	0,5 %	0,4 %
6.	Sprung-Zwillingsfehler	$xzx \to yzy$	0,3 %	0,4 %
7.	sonstige/zufällige Fehler	-	8,6 %	19,9 %

Wir haben eine ähnliche Untersuchung bei einem Datenbestand von ca. 16.000 Adressen des ehemaligen Marburger Telekommunikationsunternehmens TelDaFax durchgeführt. Dabei wurde die per Telefon erfragte fünfstellige Postleitzahl der Kunden mit den richtigen, zur Adresse gehörenden Postleitzahlen verglichen. Die Auswertung der Tippfehler zeigt ein ähnliches Ergebnis wie das von Verhoeff. Die größere Abweichung bei den sonstigen/zufälligen Fehlern (siehe letzte Zeile der obigen Tabelle) ist dabei auf Postleitzahlen zurückzuführen, die sich seit dem Datum der Erfassung bis zum Zeitpunkt der Auswertung geändert haben. Eine weitere, allerdings weniger differenzierte Fehlerstatistik stammt von Beckley (siehe [3]). Er kommt auf eine relative Häufigkeit der Einzelfehler von 86%, der Fehlerarten 2 und 3 von 8% und der restlichen von 6%.

Ein Prüfzifferverfahren sollte daher zumindest alle Einzelfehler und Nachbarvertauschungen erkennen.

1.2 Prüfziffern

Im folgenden betrachten wir einige aktuelle Beispiele für den praktischen Einsatz von Prüfziffern. Eine Reihe weiterer Beispiele findet man in [18], [53] und [57].

1.2.1 Euro-Seriennummern

Während bei den DM-Banknoten ein aufwendiges Verfahren basierend auf der Diedergruppe zur Berechnung der Prüfziffer angewendet wurde, wird bei den Euro-Seriennummern einfach die Quersumme Modulo 9 genommen (siehe [57]). Dabei nimmt man in Kauf, dass sowohl bestimmte Einzelfehler als auch alle Nachbarvertauschungen nicht erkannt werden.

Als Beispiel dient uns die Seriennummer X 1519507901 9. Der Buchstabe gibt das Land an, in dem die Banknote hergestellt wurde (siehe Tabelle). Dieser wird

Kennbuchstabe	Position im Alphabet +10	Land
Z	36	Belgien
Y	35	Griechenland
X	34	Deutschland
(W)	33	(Dänemark)
V	32	Spanien
U	31	Frankreich
T	30	Irland
S	29	Italien
R	28	Luxemburg
P	26	Niederlande
N	24	Österreich
M	23	Portugal
L	22	Finnland
(K)	21	(Schweden)
(J)	20	(Großbritannien)

Abbildung 1.1: Kennbuchstaben der Euro-Seriennummern

zunächst gemäß der Position im Alphabet in eine Zahl umgerechnet. Danach wird die Quersumme über alle Ziffern modulo 9 bestimmt. Bei einer gültigen Seriennummer ist dieser Rest gleich 0, wobei die 0 als letzte Ziffer bzw. als Prüfziffer ausgeschlossen wird.

In unserem Beispiel erhalten wir:

$$3+4+1+5+1+9+5+0+7+9+0+1+9 = 54 \equiv 0 \mod 9$$

Da $\mathbb{Z}_9$ abelsch ist, werden Nachbarvertauschungen nicht erkannt. Ebenso wird nicht erkannt, wenn die 0 gegen die 9 vertauscht ist. Das Foto zeigt dies anhand von Original-Euro-Seriennummern.

Abbildung 1.2: Euro-Seriennummern

1.2.2 IMEI

Die International Mobile Station Equipment Identity kommt bei der Identifizierung von Mobiltelefonen zum Einsatz. Die IMEI ist eine eindeutige Nummer, über die sich das Mobiltelefon im Netz des Mobilfunkbetreibers anmeldet. Bei Diebstahl kann man über die IMEI ein Mobiltelefon sperren lassen, wodurch es für den Dieb

unbrauchbar wird. Auch hier hilft eine Prüfziffer, manuelle Übertragsfehler (z.B. beim Abschreiben der IMEI oder bei der Weitergabe per Telefon) zu erkennen. Ebenso wie bei den Euro-Seriennummern wird ein so genanntes Modulo-Verfahren benutzt, d.h. es wird in $\mathbb{Z}_n$ gerechnet. Statt $n = 9$ wird aber $n = 10$ benutzt, wodurch die Erkennung aller Einzelfehler sichergestellt wird. Als Prüfgleichung dient hier:

$$d_m + \varphi(d_{m-1}) + ... + d_2 + \varphi(d_1) + d_0 \equiv 0 \mod 10.$$

Bei der Bildung der Quersumme wird an jeder zweiten Stelle eine Permutation φ angewendet, mit $\varphi(x) = 2x$, falls $x \leq 4$, und $\varphi(x) = 2x - 9$, falls $x > 4$. Durch dieses Verfahren werden immerhin ca. 97,8% der Nachbarvertauschungen erkannt. Nur der Zahlendreher $09 \leftrightarrow 90$ bleibt unentdeckt.

1.2.3 Schweizer Einzahlungsscheine

Die Prüfziffer bei Schweizer Einzahlungsscheinen wird mit einer Quasigruppe berechnet [23]. Anhand der Verknüpfungstafel und beginnend mit 0 wird die zu sichernde Zahl von links nach rechts durchmultipliziert und das Ergebnis von 10 subtrahiert. Diese Zahl dient dann als Prüfziffer (bei 10 wird 0 als Prüfziffer genommen). Die Prüfgleichung ist also

$$(...((0 * d_m) * d_{m-1})...) * d_1 + d_0 \equiv 0 \mod 10,$$

wobei mit der folgenden Verknüpfungstafel, die eine Quasigruppe darstellt, gerechnet wird:

$*$	0	1	2	3	4	5	6	7	8	9
0	0	9	4	6	8	2	7	1	3	5
1	9	4	6	8	2	7	1	3	5	0
2	4	6	8	2	7	1	3	5	0	9
3	6	8	2	7	1	3	5	0	9	4
4	8	2	7	1	3	5	0	9	4	6
5	2	7	1	3	5	0	9	4	6	8
6	7	1	3	5	0	9	4	6	8	2
7	1	3	5	0	9	4	6	8	2	7
8	3	5	0	9	4	6	8	2	7	1
9	5	0	9	4	6	8	2	7	1	3

Für den abgebildeten Einzahlungsschein (Abbildung 1.3) gilt z.B.

$$((\ldots((0*0)*1)*0)*9)*7)*9)*2)*8)*9)*9)*9)*9)*0)*0)*1)+3 \equiv 0 \mod 10.$$

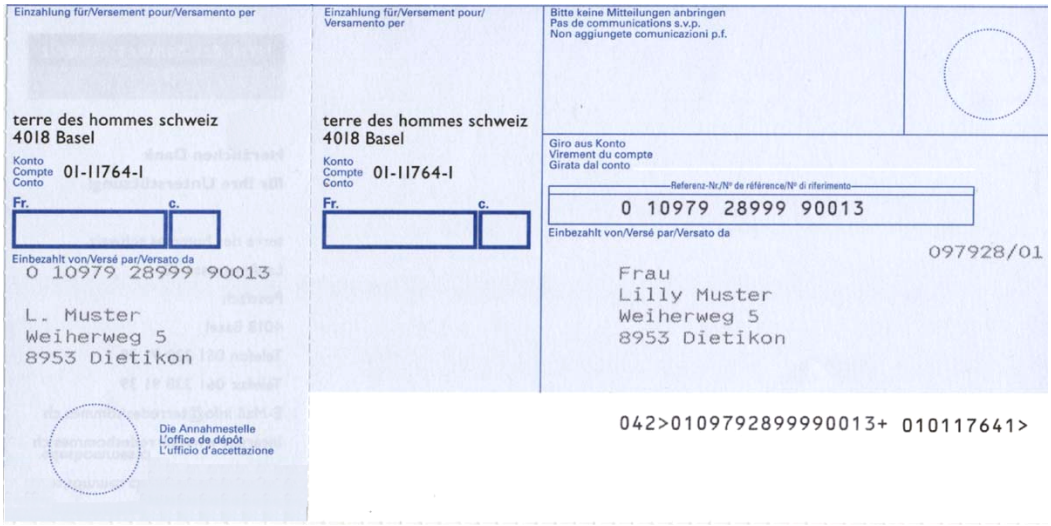

Abbildung 1.3: Schweizer Einzahlungsschein

Auch dieses Verfahren erkennt alle Einzelfehler, jedoch nicht alle Nachbarvertauschungen. Der Zahlendreher 318... $\leftrightarrow$ 381... wird z.B. nicht erkannt, wodurch

$$0031801234567895$$

und

$$0038101234567895$$

gültige Nummern sind.

(Später wird sich die Frage stellen, ob die benutzte Quasigruppe (schwach) total anti-symmetrisch ist. Unabhängig davon, dass nicht alle Nachbarvertauschungen erkannt werden, lässt sie sich mit Lemma 7.2 und anhand der Verknüpfungstafel recht leicht beantworten. Die Spaltenpermutationen $q_i : x \mapsto x * i$ einer total anti-symmetrischen Quasigruppe besitzen genau einen Fixpunkt. Dies trifft aber hier nicht zu, q_1 z.B. hat keinen und q_6 zwei Fixpunkte 1 und 8.)

Kapitel 2

Prüfziffersysteme

Ein Prüfziffersystem (oder auch Prüfzeichensystem genannt) ist ein Verfahren zur Berechnung einer Prüfziffer aus einer vorgegebenen Zahlen- oder Zeichenfolge. Die wohl am meisten benutzten Prüfziffersysteme sind die so genannten Modulo-Verfahren, die auf der zyklischen Gruppe $\mathbb{Z}_n$ basieren. Dabei wird die Prüfziffer d_0 durch eine gewichtete Summe

$$d_0 := a_m d_m + a_{m-1} d_{m-1} + \ldots + a_1 d_1$$

berechnet, mit $a_i \in \mathbb{Z}_n$.

Die Deutsche Post AG benutzt z.B. die Gewichte $a_i = 6$, falls i ungerade, und $a_i = 1$, falls i gerade ist, mit Rechnung in $\mathbb{Z}_{10}$, um den Ident- und den Leitcode der Pakete zu sichern. Mit diesen Gewichten können zwar fast alle Nachbarvertauschungen erkannt werden, aber jetzt werden nicht mehr alle Einzelfehler erkannt. Da 6 nicht teilerfremd zu 10 ist, gilt $6 \cdot 5 = 6 \cdot 0$, d.h. es werden an allen ungeraden Positionen Verwechslungen von 5 mit 0, 1 mit 6 und so weiter nicht erkannt.

Auch die Wahl anderer Gewichte führt nicht dazu, dass sowohl alle Einzelfehler als auch alle Nachbarvertauschungen erkannt werden. Um die Einzelfehler erkennen zu können, müssen die Gewichte teilerfremd zu 10 sein. Dies führt aber dazu, dass $(a_i - a_{i-1})$ gerade ist, also ist $(a_i - a_{i-1})$ nicht teilerfremd zu 10 und alle Vertauschungen der Form $x_m \ldots x_i x_{i-1} \ldots x_1 \rightarrow x_m \ldots x_{i-1} x_i \ldots x_1$ bleiben unerkannt, wenn $(x_i - x_{i-1}) \equiv 5 \mod 10$. Wie wir später sehen werden, wird das Problem auch nicht durch den allgemeineren Ansatz gelöst, bei dem statt der Multiplikation mit einem Element a_i eine Permutation auf die einzelnen Ziffern angewendet wird.

Die Notwendigkeit, dass sowohl die Gewichte als auch die Differenzen benachbarter Gewichte teilerfremd zu n sein müssen, führt auf den Gedanken, eine Primzahl als Modulus zu benutzen. Die zur 10 nächste Primzahl ist die 11, so dass beim Rechnen in der Gruppe $\mathbb{Z}_{11}$ die Schwierigkeiten bei der Suche nach geeigne-

ten Gewichten zur Fehlererkennung nicht auftreten. Es reicht vielmehr aus, dass benachbarte Gewichte verschieden sind und im Bereich von 1 bis 10 liegen, um alle Einzelfehler und Nachbarvertauschungen zu erkennen. Ein bekanntes Beispiel einer Modulo-11-Prüfung stellen die Internationalen Standard Buchnummern (ISBN) dar. Ein gravierender Nachteil bei den Modulo-11-Verfahren ist, dass beim Rechnen der Rest (die Prüfziffer) 10 herauskommen kann. Es gibt verschiedene Möglichkeiten, mit diesem Problem umzugehen. Man kann etwa bei einem Rest von 10 ein nicht-numerisches Zeichen als Ersatz nehmen. So wird z.B. bei den ISBN-Prüfziffern ein „X“ als elfte Ziffer benutzt. Eine weitere Möglichkeit besteht darin, alle Zahlen, bei denen als Prüfziffer die 10 entsteht, nicht zu verwenden. Laut Ecker und Poch [24] verfährt die Dresdner Bank auf diese Weise.

Im Normalfall sollen die Prüfziffern allerdings aus den gleichen Ziffern bestehen wie die zu sichernde Zahl. Häufig möchte man auch nicht auf eine fortlaufende Vergabe der Zahlen verzichten. In den meisten Fällen ist daher das Modulo-11-Verfahren unbrauchbar. Als Alternative bietet sich die zweite Gruppe mit 10 Elementen an, nämlich die Diedergruppe. Prüfzifferverfahren basierend auf Diedergruppen bieten ebenfalls eine sehr gute Fehlererkennung, z.B. wurden die Seriennummern der DM-Banknoten damit gesichert.

2.1 Prüfziffersysteme über Gruppen

Die einfachste Methode zur Berechnung der Prüfziffer d_0 mit einer Gruppe $(G, \cdot)$ ist, alle Elemente miteinander zu multiplizieren:

$$d_0 := d_{m-1} \cdot d_{m-2} \cdot \ldots \cdot d_1.$$

Dies kommt, wie wir gesehen haben, zum Beispiel bei den Seriennummern der Eurobanknoten zum Einsatz. Allgemeiner werden vor der Produktbildung Permutationen τ_i auf die einzelnen Stellen angewendet (vergleiche Schulz [57]), d.h.

$$\tau_m(d_m) \cdot \tau_{m-1}(d_{m-1}) \cdot \ldots \cdot \tau_1(d_1) \cdot \tau_0(d_0) = c$$

mit $c \in G$ fest gewählt. Da wir die Prüfgleichung nach d_0 auflösen können, existiert für alle $d_m, \ldots, d_1$ eine Lösung. Es ist für die Erkennung aller Einzelfehler erforderlich, dass die τ_i injektiv, bzw. im endlichen Fall Permutationen sind, denn

$$\begin{array}{lrcl} & \tau_m(d_m) \cdot \ldots \cdot \tau_i(d_i) \cdot \ldots \cdot \tau_0(d_0) & = & \tau_m(d_m) \cdot \ldots \cdot \tau_i(d_i') \cdot \ldots \cdot \tau_0(d_0) \\ \Leftrightarrow & \tau_i(d_i) & = & \tau_i(d_i') \\ \Leftrightarrow & d_i & = & d_i' \end{array}$$

Damit die Transpositionen erkannt werden, darf die folgende Gleichung nur für $d_i = d_{i-1}$ gelten:

$$\begin{aligned} & \tau_m(d_m) \cdot \ldots \cdot \tau_i(d_i) \cdot \tau_{i-1}(d_{i-1}) \cdot \ldots \cdot \tau_0(d_0) \quad = \\ & \qquad\qquad \tau_m(d_m) \cdot \ldots \cdot \tau_i(d_{i-1}) \cdot \tau_{i-1}(d_i) \cdot \ldots \cdot \tau_0(d_0) \\ \Leftrightarrow \quad & \tau_i(d_i) \cdot \tau_{i-1}(d_{i-1}) \quad = \quad \tau_i(d_{i-1}) \cdot \tau_{i-1}(d_i) \\ \Leftrightarrow \quad & \tau_i \circ \tau_{i-1}^{-1}(\tau_{i-1}(d_i)) \cdot \tau_{i-1}(d_{i-1}) \quad = \quad \tau_i \circ \tau_{i-1}^{-1}(\tau_{i-1}(d_{i-1})) \cdot \tau_{i-1}(d_i). \end{aligned}$$

Dies ist aber genau dann der Fall, wenn $\tau_i \circ \tau_{i-1}^{-1}(x) \cdot y = \tau_i \circ \tau_{i-1}^{-1}(y) \cdot x \Rightarrow x = y$ gilt. Wie wir sehen, spielen hier die Permutationen φ, bei denen aus $\varphi(x) \cdot y = \varphi(y) \cdot x$ die Gleichheit von x und y folgt, eine wichtige Rolle. Diese werden *anti-symmetrisch* genannt. Sie sind erforderlich für die Existenz eines Prüfziffersystems über einer Gruppe. Andererseits kann man mit ihnen auch ein Prüfziffersystem definieren (vgl. H.P. Gumm [28]):

Sei φ eine anti-symmetrische Permutation der Gruppe G, dann wird durch $\tau_i := \varphi^i$, ein beliebiges Element $c \in G$, sowie die Kontrollgleichung

$$\varphi^m(x_m) \cdot \varphi^{m-1}(x_{m-1}) \cdot \ldots \cdot \varphi(x_1) \cdot x_0 = c$$

ein Prüfziffersystem definiert.

2.1.1 Abelsche Gruppen

In abelschen Gruppen stehen die anti-symmetrischen Abbildungen in direkter Beziehung zu den von Mann [41] 1942 eingeführten vollständigen Abbildungen. Eine Permutation φ heißt vollständig, wenn $x \cdot \varphi(x) = y \cdot \varphi(y)$ impliziert, dass $x = y$ ist (also wenn $x \cdot \varphi(x)$ wieder eine Permutation ist). Mit Hilfe der vollständigen Abbildungen ist es möglich, orthogonale lateinische Quadrate zu konstruieren.

Man kann sich leicht klar machen, dass eine abelsche Gruppe genau dann eine vollständige Abbildung besitzt, wenn sie eine anti-symmetrische Abbildung besitzt. Die Frage, wann eine endliche abelsche Gruppe eine vollständige Abbildung besitzt, wurde von Paige 1947 gelöst.

Theorem 2.1 *(Paige* [49]*) Eine endliche abelsche Gruppe der Ordnung n besitzt eine vollständige und damit eine anti-symmetrische Abbildung genau dann, wenn n ungerade ist oder wenn G mindestens zwei verschiedene Involutionen enthält (also die 2-Sylowgruppe von G nicht zyklisch ist).*

Damit gilt, dass eine zyklische Gruppe $\mathbb{Z}_n$ der Ordnung n genau dann eine anti-symmetrische Abbildung besitzt, wenn n ungerade ist. Über den Gruppen $\mathbb{Z}_{2k}$, $k \geq 1$, insbesondere über $\mathbb{Z}_{10}$, existiert daher kein Prüfziffersystem. Die Gruppe $\mathbb{Z}_{10}$ eignet sich also grundsätzlich nicht dazu, ein Prüfziffersystem zu definieren.

2.1.2 Diedergruppe

Die Diedergruppe D_n der Ordnung $2n$ ist die Gruppe der n Drehungen und n Spiegelungen, die ein regelmäßiges n-Eck auf sich selbst abbilden. Sie spielt eine wichtige Rolle in Verbindung zu Prüfziffersystemen, da sie die einzige Gruppe der Ordnung 10 ist, die eine anti-symmetrische Abbildung besitzt und damit die Definition eines Prüfziffersystems zulässt. Von Gumm [28] stammt das Ergebnis, dass D_n für n ungerade eine anti-symmetrische Abbildung hat. Gallian und Mullin [27] verallgemeinerten dies auf beliebige Diedergruppen D_n mit $n \geq 3$. Stellt man sich nun die Frage, wie die Fehlererkennung der anderen wichtigen Fehlerarten ist, so haben wir in [18] festgestellt:

Theorem 2.2 *Sei $n \geq 3$ ungerade. Über der Diedergruppe D_n existiert kein Prüfziffersystem, das alle Sprung-Transpositionen oder alle (Sprung-)Zwillingsfehler erkennt.*

Da die Gruppe $\mathbb{Z}_{10}$ keine anti-symmetrische Abbildung besitzt, existiert kein Prüfziffersystem über einer Gruppe der Ordnung 10, welches alle Sprung-Transpositionen oder alle (Sprung-)Zwillingsfehler erkennt. Da Gruppen der Ordnung $4k+2$ keine vollständige Abbildung besitzen (siehe Simon [61]), kann ein Prüfziffersystem über einer Gruppe der Ordnung $4k+2$ grundsätzlich nicht alle (Sprung-) Zwillingsfehler erkennen.

2.2 Verallgemeinerung

Wie wir gesehen haben, können wir mit einem Prüfziffersystem über einer Gruppe der Ordnung 10 grundsätzlich nicht alle Fehlerarten erkennen. Da wir für die Berechnung der Prüfziffer nicht unbedingt die Assoziativität einer Gruppe benötigen, können wir einen allgemeineren Ansatz mit n-Quasigruppen untersuchen. Eine n-Quasigruppe ist eine Menge Q mit einer Operation $f : Q^n \mapsto Q$, so dass für $i = 1, \ldots, n$ und alle $x_n, \ldots, x_1, x_0 \in Q$ die Gleichung $f(x_n, \ldots, x_{i+1}, x, x_{i-1}, \ldots, x_1) = x_0$ eine eindeutig bestimmte Lösung $x \in Q$ besitzt.

Die statistische Häufigkeit der einzelnen Fehlerarten legt es nahe, dass wir zumindest die Erkennung von Einzelfehlern und Transpositionen verlangen. Außerdem soll zu einer vorgegebenen Zahl eine gesicherte Zahl existieren. Dies motiviert folgende Definition (vgl. H.P. Gumm [28]).

Definition 2.1 *Sei $D = \{0, \ldots, m-1\}$ eine Menge von Ziffern und $f : D^n \to D$ eine Abbildung. Die Menge $P_f := \{(d_n, \ldots, d_0) \in D^{n+1} | f(d_n, \ldots, d_1) = d_0\}$ heißt* Prüfziffersystem zur Basis m, *wenn gilt:*

1. $f(d_n, \ldots, d_i, \ldots, d_1) = f(d_n, \ldots, d'_i, \ldots, d_1)$ *impliziert* $d_i = d'_i$
2. $f(d_n, \ldots, d_i, d_{i-1}, \ldots, d_1) = f(d_n, \ldots, d_{i-1}, d_i, \ldots, d_1)$ *impliziert* $d_i = d_{i-1}$
3. $f(d_n, \ldots, d_2, d_0) = d_1$, *wobei* $f(d_n, \ldots, d_1) = d_0$, *impliziert* $d_0 = d_1$

Die erste Eigenschaft garantiert die Erkennung der Einzelfehler, die zweite sorgt für das Erkennen aller Nachbarvertauschungen. Die dritte Eigenschaft dient schließlich dazu, die Vertauschung der letzten Ziffer mit der Prüfziffer zu erkennen.

Neben dieser expliziten gibt es noch eine implizite Darstellung, bei der sich die Prüfziffer als eindeutige Lösung einer Gleichung ergibt. Dazu sei $c \in D$ und $f : D^{n+1} \to D$ eine Abbildung. Zu einer vorgegebenen Zahl $d_n, \ldots, d_1$ wird d_0 so bestimmt, dass $f(d_n, \ldots, d_1, d_0) = c$ gilt. Dabei setzen wir voraus, dass es immer eine solche Lösung d_0 gibt und außerdem f die Eigenschaften (1) und (2) besitzt. Die dritte Eigenschaft wird dabei nicht benötigt. Das Prüfziffersystem ist dann durch die Menge

$$P_f := \{(d_n, \ldots, d_0) \in D^{n+1} | f(d_n, \ldots, d_1, d_0) = c\}$$

definiert.

Beide Darstellungen lassen es auch zu, eine Prüfziffer zu bestimmen, die in die ursprüngliche Zahl an einer Position i eingebaut wird. Dazu bestimmt man die eindeutige Lösung p der Gleichung

$$f(d_n, \ldots, d_{i+1}, p, d_i, \ldots, d_2) = d_1$$

bzw.

$$f(d_n, \ldots, d_{i+1}, p, d_i, \ldots, d_1) = c.$$

Die gesicherte Zahl lautet in beiden Fällen $d_n d_{n-1} \ldots d_{i+1} p d_i \ldots d_2 d_1$.

2.3 Prüfziffersysteme über Quasigruppen

Betrachten wir die erste Eigenschaft von Definition 2.1 für den Fall $n = 2$, so gilt für f:

$$f(d_2, d_1) = f(d_2, d'_1) \Rightarrow d_1 = d'_1$$
$$f(d_2, d_1) = f(d'_2, d_1) \Rightarrow d_2 = d'_2.$$

Das heißt, f ist eine 2-stellige Operation auf D, für die die Kürzungsregeln gelten. Damit ist (D, f), weil D endlich ist, eine Quasigruppe und für den höher dimensionalen Fall $n > 2$ eine n-Quasigruppe.

Umgekehrt kann man mit Quasigruppen, die bestimmte Eigenschaften besitzen, ein Prüfziffersystem definieren. Dazu seien $(Q, *_i)$, $i = 0, 1, 2, \ldots, n-1$ Quasigruppen auf der Menge $Q = \{0, 1, \ldots, m-1\}$ und

$$f(d_n, d_{n-1}, \ldots, d_1, d_0) := ((\ldots(d_n *_{n-1} d_{n-1}) *_{n-2} \ldots) *_1 d_1) *_0 d_0.$$

f erfüllt Bedingung (1) der Definition 2.1. Bedingung (2) gilt genau dann, wenn für alle i und alle $c, x, y \in Q$ gilt:

$$\begin{aligned} x *_{n-1} y = y *_{n-1} x \quad &\Rightarrow \quad x = y \\ (c *_{i+1} x) *_i y = (c *_{i+1} y) *_i x \quad &\Rightarrow \quad x = y. \end{aligned}$$

Bedingung (3) ist erfüllt, wenn für alle $x, y \in Q$ gilt:

$$x *_0 (x *_0 y) = y \quad \Rightarrow \quad x *_0 y = y.$$

Wählen wir alle Quasigruppen $(Q, *_i)$ gleich zu einer Quasigruppe $(Q, *)$, so führt uns dies auf die so genannten *total anti-symmetrischen* Quasigruppen. Wir nennen eine Quasigruppe $(Q, *)$ total anti-symmetrisch, wenn für alle $c, x, y \in Q$ gilt:

$$\begin{aligned} (c * x) * y = (c * y) * x \quad &\Rightarrow \quad x = y \\ x * y = y * x \quad &\Rightarrow \quad x = y. \end{aligned}$$

Ist $(Q, *)$ eine total anti-symmetrische Quasigruppe, dann definiert

$$f(d_n, d_{n-1}, d_{n-2}, \ldots, d_1, d_0) := ((\ldots((d_n * d_{n-1}) * d_{n-2}) * \ldots) * d_1) * d_0 = 0$$

ein (implizites) Prüfziffersystem. Bei dieser Darstellung können wir auf Bedingung (3) verzichten.

Bevor wir uns mit der Frage beschäftigen können, ob wir mit TA-Quasigruppen weitere Fehlerarten vollständig erkennen können, ist erst einmal zu klären, ob es überhaupt solche Quasigruppen gibt. Diesem Problem stellen wir uns ausführlich im Kapitel „Total anti-symmetrische Quasigruppen“.

Kapitel 3

Quasigruppen

Dieser Abschnitt soll eine kleine Einführung in die Theorie der Quasigruppen sein. Wir führen hier die wichtigsten Begriffe und Ergebnisse auf, die für die Betrachtung der Prüfziffersysteme und der damit verbundenen total anti-symmetrischen Quasigruppen notwendig sind.

3.1 Universell algebraische Begriffe

Wir beginnen mit den Grundlagen der universellen Algebra. Die universelle Algebra hat zum Ziel, so weit wie möglich die gemeinsamen Elemente verschiedener algebraischer Strukturen herauszuarbeiten. Dies bringt nicht nur Verallgemeinerungen und Vereinheitlichungen, sondern ermöglicht es auch, die Ergebnisse auf neue Situationen zu übertragen.

Die folgende Definition einer Algebra deckt fast alle bekannten algebraischen Strukturen ab, ebenso eine große Anzahl weniger bekannter Algebren, die Gegenstand der aktuellen Forschung sind.

3.1.1 Definitionen

Definition 3.1 *Sei A eine Menge und $n \in \mathbb{N} \cup \{0\}$, so heißen die Abbildungen $f : A^n \to A$* n-stellige Operationen *auf A und n ihre Stelligkeit.*

Die 0-stelligen Operationen sind die konstanten Funktionen $f_a : \emptyset \to \{a\}$, die genau den Elementen der Grundmenge A entsprechen.

Definition 3.2 *Unter einem* Typ *versteht man ein geordnetes Paar $(\mathcal{F}, \sigma)$, wobei $\mathcal{F}$ eine Menge (von Operationssymbolen) ist und $\sigma : \mathcal{F} \to \mathbb{N} \cup \{0\}$ jedem $f \in \mathcal{F}$ seine Stelligkeit $\sigma(f)$ zuordnet.*

Eine allgemeine Algebra *(oder kurz:* Algebra*) vom Typ* $(\mathcal{F}, \sigma)$ *ist ein geordnetes Paar* (A, F)*, bestehend aus einer Menge* A *und einer Familie* $F = (f^A | f \in \mathcal{F})$ *von Operationen auf* A*, wobei jedem Operationssymbol* $f \in \mathcal{F}$ *eine* $\sigma(f)$*-stellige Operation* f^A *zugeordnet wird.*

Besteht die Menge F der Operationen einer Algebra (A, F) aus nur endlich vielen Elementen, so schreiben wir $(A, f_1, \ldots, f_k)$ anstatt (A, F). Den Typ notieren wir in diesem Fall in der Form $(\sigma_1, \ldots, \sigma_k)$.

Definition 3.3 *Sei* (A, F) *eine Algebra vom Typ* $(\mathcal{F}, \sigma)$ *und* $B \subset A$ *eine Teilmenge. Mit* $f^B : B^n \to B$ *bezeichnen wir die Einschränkung von* f^A *auf die Menge* B*. Die Algebra* $(B, (f^B | f \in \mathcal{F}))$ *heißt* Unteralgebra *von* A*, falls für alle* n *und alle* $f \in \mathcal{F}$ *mit* $\sigma(f) = n$ *und alle* n*-Tupel* $(b_1, \ldots, b_n) \in B^n$

$$f^A(b_1, \ldots, b_n) \in B$$

gilt.

Definition 3.4 *Seien* $\mathcal{A} = (A, F_\mathcal{A})$ *und* $\mathcal{B} = (B, F_\mathcal{B})$ *Algebren vom selben Typ* $(\mathcal{F}, \sigma)$ *und* $\varphi : A \to B$ *eine Abbildung.* φ *heißt* Homomorphismus *von* $\mathcal{A}$ *nach* $\mathcal{B}$*, wenn für alle* n *und alle* $f \in \mathcal{F}$ *mit* $\sigma(f) = n$ *und alle* n*-Tupel* $(a_1, \ldots, a_n) \in A^n$ *gilt:*

$$\varphi(f^A(a_1, \ldots, a_n)) = f^B(\varphi(a_1), \ldots, \varphi(a_n)).$$

Ist φ *bijektiv, so nennen wir* φ Isomorphismus*. Ist* φ *surjektiv so nennen wir die Algebra* $\mathcal{B}$ *das* homomorphe Bild *von* $\mathcal{A}$*.*

Definition 3.5 *Sei* A *eine Menge.* $R \subset A^n$ *heißt* n-stellige Relation *auf* A*. Eine 2-stellige Relation* Θ *heißt* Äquivalenzrelation*, falls für alle* $x, y, z \in A$ *gilt:*

- $(x, x) \in \Theta$*,* Θ *ist reflexiv*
- $(x, y) \in \Theta \Rightarrow (y, x) \in \Theta$*,* Θ *ist symmetrisch*
- $(x, y), (y, z) \in \Theta \Rightarrow (x, z) \in \Theta$*,* Θ *ist transitiv.*

Für jede Menge A erhält man die Äquivalenzrelationen $\nabla_A := A^2$ (Allrelation) und $\Delta_A := \{(a, a) | a \in A\}$ (Diagonale). Die Schnittmenge $\Theta \cap \Psi$ zweier (Äquivalenz-)Relationen ist wieder eine (Äquivalenz-)Relation, und mit

$$\Theta \circ \Psi := \{(x, y) | \exists z \in A : (x, z) \in \Theta, (z, y) \in \Psi\}$$

bezeichnen wir das *Relationenprodukt.*

Für jede Aquivalenzrelation Θ heißen die Mengen der Form $[a]\Theta := \{x \in A | (x, a) \in \Theta\}$ *Äquivalenzklassen.* Eine *Kongruenzrelation* ist eine Äquivalenzrelation, für die für jede n-stellige Operation f^A aus $(a_1, b_1), \ldots, (a_n, b_n) \in \Theta$ folgt:

$$(f^A(a_1, \ldots, a_n), f^A(b_1, \ldots, b_n)) \in \Theta.$$

Zu einer Algebra (A, F) mit der Kongruenzrelation Θ wird die *Faktoralgebra* $(A/\Theta, F)$ auf der Menge der Äquivalenzklassen $A/\Theta := \{[a]\Theta | a \in A\}$ definiert durch die Operationen

$$f^{A/\Theta}([a_1]\Theta, \ldots, [a_n]\Theta) := [f^A(a_1, \ldots, a_n)]\Theta.$$

Definition 3.6 *Seien $\mathcal{A} = (A, F_\mathcal{A})$ und $\mathcal{B} = (B, F_\mathcal{B})$ Algebren desselben Typs. Das* direkte Produkt *(oder* Kreuzprodukt*) $\mathcal{A} \times \mathcal{B} = (A \times B, F_{\mathcal{A}\times\mathcal{B}})$ der Algebren $\mathcal{A}$ und $\mathcal{B}$ ist für jedes $f \in \mathcal{F}$ definiert durch*

$$f^{A\times B}((a_1, b_1), \ldots, (a_n, b_n)) := (f^A(a_1, \ldots, a_n), f^B(b_1, \ldots, b_n)),$$

wobei $\sigma(f) = n$ ist.

Man kann sich leicht klar machen, dass sich eine Implikation (z.B. $x \cdot y = y \cdot x \Rightarrow x = y$), die in $\mathcal{A}$ und $\mathcal{B}$ gilt, auf das direkte Produkt überträgt. Selbstverständlich kann man auch direkte Produkte aus mehr als zwei, sogar aus unendlich vielen, Algebren bilden. Dazu seien $\mathcal{A}_i$, $i \in I$, Algebren desselben Typs. Dann ist das direkte Produkt $\prod_{i\in I} \mathcal{A}_i$ definiert durch die Grundmenge $\prod_{i\in I} A_i$ und den für jedes $f \in \mathcal{F}$ mit $\sigma(f) = n$ komponentenweise definierten Operationen

$$f^{\prod A_i}(a_1, \ldots, a_n)^{(j)} := f^{A_i}(a_1^{(j)}, \ldots, a_n^{(j)})$$

für alle $j \in I$ und $a_1, \ldots, a_n \in \prod_{i\in I} A_i$. Dabei bezeichnen wir die j-te Komponente von $a \in \prod_{i\in I} A_i$ mit $a^{(j)}$.

Definition 3.7 *Eine Klasse von Algebren desselben Typs heißt* Varietät*, wenn sie unter der Bildung von Unteralgebren, homomorphen Bildern und direkten Produkten abgeschlossen ist.*

Ein berühmter Satz von G. Birkhoff [7] besagt, dass eine Klasse von Algebren genau dann gleichungsdefiniert ist (sich also durch Gleichungen beschreiben lässt), wenn sie eine Varietät ist.

3.1.2 Quasigruppen, Gruppen, Ringe

Ein bekanntes Beispiel für eine gleichungsdefinierte Klasse von Algebren sind Gruppen:

Definition 3.8 *Eine* Gruppe *ist eine Algebra* $(G, \cdot, ^{-1}, e)$ *vom Typ* $(2, 1, 0)$*, die den folgenden Axiomen genügt:*

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
2. $e \cdot x = x \cdot e = x$,
3. $x \cdot x^{-1} = x^{-1} \cdot x = e$.

Eine Gruppe heißt abelsch *oder* kommutativ*, falls gilt:*

4. $x \cdot y = y \cdot x$.

In abelschen Gruppen ist es üblich, die additive Schreibweise $+, -, 0$ anstelle von $\cdot, ^{-1}, e$ zu benutzen.

Definition 3.9 *Sei* $(Q, *, /, \backslash)$ *eine Algebra vom Typ* $(2, 2, 2)$*. Q heißt* Quasigruppe*, wenn gilt:*

1. $x * (x\backslash y) = y$ *und* $x\backslash(x * y) = y$,
2. $(x * y)/y = x$ *und* $(x/y) * y = x$.

Gibt es ein Element $e \in Q$, so dass für alle $x \in Q$ gilt: $e * x = x$ (bzw. $x * e = x$), so heißt $(Q, *, /, \backslash, e)$ Links-Loop (bzw. Rechts-Loop). $(Q, *)$ heißt Loop, wenn für ein $e \in Q$ gilt: $e * x = x * e = x$.

Damit ist die Klasse der Gruppen bzw. Quasigruppen gleichungsdefiniert und bildet somit eine Varietät, ist also unter der Produktbildung, homomorphen Bildern und Unteralgebren abgeschlossen.

Definition 3.10 *Ein* Ring *ist eine Algebra* $(R, +, -, 0, \cdot)$ *vom Typ* $(2, 1, 0, 2)$*, wenn* $(R, +, -, 0)$ *eine abelsche Gruppe ist und wenn gilt*

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
2. $x \cdot (y + z) = x \cdot y + x \cdot z$,
3. $(x + y) \cdot z = x \cdot z + y \cdot z$.

Er heißt kommutativ*, wenn $x \cdot y = y \cdot x$. Ein Ring mit Einselement (kurz: Ring mit Eins) ist eine Algebra $(R, +, -, 0, \cdot, 1)$, wobei $(R, +, -, 0, \cdot)$ ein Ring ist und $1 \cdot x = x \cdot 1 = x$ gilt.*

Statt $(R, +, -, 0, \cdot)$ bzw. $(R, +, -, 0, \cdot, 1)$ schreiben wir auch kurz $(R, +, \cdot)$. Ein Element $r \in R\backslash\{0\}$ eines kommutativen Rings mit Eins heißt *Nullteiler*, falls es ein $s \in R\backslash\{0\}$ gibt mit $r \cdot s = 0$. $r \in R$ heißt *Einheit*, wenn es ein $s \in R$ gibt mit $r \cdot s = 1$. Ist R endlich, so lassen sich die Elemente von R in die Null, die Einheiten und die Nullteiler partitionieren. Im unendlichen Fall gilt dies im Allgemeinen nicht. Im Ring der ganzen Zahlen $(\mathbb{Z}, +, \cdot)$ ist die 2 z.B. weder Einheit noch Nullteiler.

3.2 Kombinatorische Betrachtung

Oft wird eine Quasigruppe auch alternativ zu Definition 3.9 als eine Algebra $(Q, *)$ mit einer 2-stelligen Operation definiert:

Definition 3.11 *Eine Quasigruppe ist eine Algebra $(Q, *)$ mit der Eigenschaft, dass die Gleichungen $a * x = b$ und $y * a = b$ für jedes Paar $a, b \in Q$ eine eindeutige Lösung x bzw. y aus Q besitzen.*

Eine n-Quasigruppe ist eine Algebra (Q, f), $f : Q^n \to Q$, so dass für $i = 1, \ldots, n$ und alle $x_n, \ldots, x_{i+1}, x_{i-1}, \ldots, x_1, x_0 \in Q$ die Gleichung

$$f(x_n, \ldots, x_{i+1}, x, x_{i-1}, \ldots, x_1) = x_0$$

eine eindeutig bestimmte Lösung $x \in Q$ besitzt.

Als Nachweis dafür, dass die vorherige Definition dieser entspricht, verifiziert man x/y als eindeutige Lösung z_1 der Gleichung $z_1 * y = x$ und $z_2 = x\backslash y$ als eindeutige Lösung von $x * z_2 = y$.

Gilt in einer Quasigruppe das Assoziativgesetz $(x * y) * z = x * (y * z)$, so ist sie bereits eine Gruppe. Anders ausgedrückt: Gruppen sind genau die assoziativen Quasigruppen.

Quasigruppen sind eng mit lateinischen Quadraten verbunden. Ein lateinisches Quadrat ist eine $n \times n$-Matrix über einer n-elementigen Menge, so dass in jeder Zeile und in jeder Spalte kein Element mehr als einmal vorkommt. Die Verknüpfungstafel (ohne Rand) einer Quasigruppe ist ein lateinisches Quadrat und umgekehrt kann jedes lateinische Quadrat als Verknüpfungstafel einer Quasigruppe angesehen werden:

0	1	2
2	0	1
1	2	0

lateinisches Quadrat

$*$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

Quasigruppe

Nachfolgend verwenden wir daher die Begriffe Quasigruppe und lateinisches Quadrat bzw. die Verknüpfungstafel mit und ohne Rand gleichwertig.

Vertauscht man die Zeilen oder Spalten einer Quasigruppe oder benennt man die Elemente um, so erhält man wiederum eine Quasigruppe. Das Gleiche gilt auch für den n-dimensionalen Fall. Quasigruppen, die auf diese Weise ineinander überführt werden können, nennt man isotop:

Definition 3.12 *Zwei n-Quasigruppen $(Q, f), (Q, g)$ heißen isotop, falls Bijektionen $\gamma, \beta_n, \ldots, \beta_1 : Q \to Q$ existieren mit*

$$\gamma(f(x_n, \ldots, x_1)) = g(\beta_n(x_n), \ldots, \beta_1(x_1)),$$

und sie heißen isomorph, falls $\gamma = \beta_n = \ldots = \beta_1$ gilt.

Isotopie und Isomorphie definieren jeweils eine Äquivalenzrelation auf der Menge der n-Quasigruppen.

Eine weitere Möglichkeit, aus vorhandenen Quasigruppen neue Quasigruppen zu erhalten, ergibt sich, wenn wir die Bedeutung von Zeilen, Spalten und Werten vertauschen. Dies führt auf die so genannten Parastrophien (oder auch Konjugierten) einer Quasigruppe.

Definition 3.13 *Die* Parastrophie f_α *einer n-Quasigruppe f und der Permutation $\alpha \in S_{n+1}$ wird definiert durch*

$$f_\alpha(x_{\alpha(n)}, \ldots, x_{\alpha(1)}) = x_{\alpha(0)} \quad :\Leftrightarrow \quad f(x_n, \ldots, x_1) = x_0.$$

Sie heißt hauptsächlich *wenn $\alpha(0) = 0$ ist.*

Offensichtlich sind die Parastrophien einer n-Quasigruppe wieder n-Quasigruppen. Für eine Quasigruppe $(Q, *)$ definieren wir:

$$\begin{aligned}
x *_t y = z \quad &:\Leftrightarrow \quad y * x = z \\
x \backslash y = z \quad &:\Leftrightarrow \quad y = x * z \\
x / y = z \quad &:\Leftrightarrow \quad x = z * y \\
x \backslash_t y = z \quad &:\Leftrightarrow \quad x = y * z \\
x /_t y = z \quad &:\Leftrightarrow \quad y = z * x
\end{aligned}$$

Es gilt $x\backslash(x * y) = y$, $x * (x\backslash y) = y$ und $(x * y)/y = x$, $(x/y) * y = x$ und somit ist $(Q, *, /, \backslash)$ auch eine Quasigruppe gemäß Definition 3.9.

Wir betrachten nun das Konzept der Transversalen. Bei lateinischen Quadraten wird eine Transversale definiert durch eine Menge von n Zellen, je eine aus jeder Zeile und Spalte, wobei je zwei verschiedene Zellen auch verschiedene Elemente enthalten. Um dies zu veranschaulichen, betrachten wir folgendes Beispiel. Die Zellen der Transversale sind hier umrahmt.

$*$	0	1	2	3	4
0	$\boxed{0}$	1	2	3	4
1	4	0	1	$\boxed{2}$	3
2	3	$\boxed{4}$	0	1	2
3	2	3	4	0	$\boxed{1}$
4	1	2	$\boxed{3}$	4	0

Für eine Quasigruppe definieren wir:

Definition 3.14 *Das Paar (α_2, α_1) heißt* Transversale *einer Quasigruppe $(Q, *)$, wenn α_2, α_1 und $x \mapsto \alpha_2(x) * \alpha_1(x)$ Permutationen der Menge Q sind.*

Analog nennen wir $(\alpha_n, \alpha_{n-1}, \ldots, \alpha_1)$ Transversale der n-Quasigruppe (Q, f), wenn die α_i und $x \mapsto f(\alpha_n(x), \alpha_{n-1}(x), \ldots, \alpha_1(x))$ Permutationen der Menge Q sind.

Die beiden Ansätze sind selbstverständlich äquivalent, $\alpha_1(i)$ ist die x-Koordinate des i-ten Punktes, $\alpha_2(i)$ die y-Koordinate. So ist bei diesem Beispiel $\alpha_2 = \mathrm{Id}$ und $\alpha_1 = (1 \quad 3 \quad 4 \quad 2)$. Die Darstellung ist allerdings nicht eindeutig, weil man die Elemente der Transversalen unterschiedlich durchnummerieren kann. $\alpha_2 = (1 \quad 2 \quad 4 \quad 3)$, $\alpha_1 = \mathrm{Id}$ definiert z.B. die gleiche Transversale.

Eine Quasigruppe kann mehrere verschiedene Transversalen haben. Zwei Transversalen (α_2, α_1) und (β_2, β_1) heißen *disjunkt*, wenn sie keine Zelle gemeinsam haben, d.h. wenn $(\alpha_2(x), \alpha_1(x)) \neq (\beta_2(x'), \beta_1(x'))$ für alle $x, x' \in Q$ gilt.

Besitzt eine Quasigruppe eine Zerlegung in disjunkte Transversalen, so besitzt sie ein so genanntes orthogonales Komplement (und umgekehrt):

Definition 3.15 *Die Quasigruppen $(Q, *)$ und $(Q, \cdot)$ heißen orthogonal, wenn die Paare $(x * y, x \cdot y)$ für alle $x, y \in Q$ paarweise verschieden sind. Eine Quasigruppe $(Q, *)$ heißt selbstorthogonal, wenn sie orthogonal zu $(Q, *_t)$ ist.*

Orthogonale lateinische Quadrate wurden zuerst von Euler Ende des 18. Jahrhunderts untersucht. Von ihm stammt die berühmte Vermutung, dass für alle

$n = 4k + 2$ kein Paar orthogonaler lateinischer Quadrate der Ordnung n existiert. Erst 180 Jahre später konnte seine Vermutung widerlegt werden.

Beispiel Ein Tripel paarweise orthogonaler lateinisch-griechisch-deutscher Quadrate ([6], Seite 140):

r	o	m	a		ω	σ	ε	ρ		i	l	b	e
o	r	a	m		ρ	ε	σ	ω		b	e	i	l
m	a	r	o		σ	ω	ρ	ε		e	b	l	i
a	m	o	r		ε	ρ	ω	σ		l	i	e	b

Definition 3.16 *Eine Quasigruppe $(Q, *)$ heißt* idempotent *(*unipotent*), wenn $x * x = x$ $(x * x = y * y)$ für alle $x, y \in Q$ gilt. Sie heißt* total symmetrisch *wenn $x * y$, $x\backslash y$ und x/y gleich sind. Eine total symmetrische idempotente Quasigruppe heißt* Steiner-Quasigruppe.

Steiner-Quasigruppen und die zugehörigen Steinertripelsysteme betrachten wir näher im Kapitel „Konstruktion von Quasigruppen“.

Bemerkung Steiner-Quasigruppen sind nicht zu verwechseln mit Stein-Quasigruppen. S. K. Stein [21], [62] versuchte, Gegenbeispiele zu Eulers Vermutung zu konstruieren. Er untersuchte Quasigruppen, welche die Gleichung $x*(x*y) = y*x$ erfüllen. Diese werden Stein-Quasigruppen genannt und sind selbstorthogonal.

Definition 3.17 *Eine Quasigruppe $(Q, *)$ heißt* distributiv*, wenn für alle $x, y, z \in Q$ gilt*

$$x * (y * z) = (x * y) * (x * z) \text{ links-distributiv und}$$

$$(x * y) * z = (x * z) * (y * z) \text{ rechts-distributiv.}$$

Setzt man $x = y = z$, so sieht man, dass eine distributive Quasigruppe idempotent ist.

Für die später betrachteten Konstruktionen von Quasigruppen wird es notwendig sein, gleichzeitig in verschiedenen (Restklassen-)Ringen zu rechnen. Zur Vereinfachung führen wir daher folgende Schreibweisen ein.

Statt $x \mod n$ schreiben wir auch $(x)_n$ und $(x)_n = (y)_n$ kürzen wir mit $x =_n y$ ab. Falls $|x - y| \leq n - 1$ gilt, so ist $x = y \Leftrightarrow x =_n y$.

3.3 Beispiele

Die folgenden Beispiele zeigen einige Zusammenhänge zwischen der kombinatorischen und der allgemein algebraischen Betrachtungsweise.

Beispiel 3.1 *(Belousov [4]) Alle zu einer Gruppe isotopen Quasigruppen werden charakterisiert durch die Gleichung*

$$x * (y\backslash((z/u) * v)) = ((x * (y\backslash z))/u) * v.$$

Beweis Die Quasigruppe $(Q, *)$ sei isotop zur Gruppe $(Q, \cdot)$, d.h.

$$x * y = \gamma^{-1}(\alpha(x) \cdot \beta(y)).$$

Es folgt

$$x\backslash z = \beta^{-1}(\alpha(x)^{-1} \cdot \gamma(z)),$$

$$z/y = \alpha^{-1}(\gamma(z) \cdot \beta(y)^{-1})$$

und damit

$$\begin{aligned}
x * (y\backslash((z/u) * v)) &= x * (y\backslash\gamma^{-1}(\alpha(z/u) \cdot \beta(v))) \\
&= x * (y\backslash\gamma^{-1}(\gamma(z) \cdot \beta(u)^{-1} \cdot \beta(v))) \\
&= x * \beta^{-1}(\alpha(y)^{-1} \cdot \gamma(z) \cdot \beta(u)^{-1} \cdot \beta(v)) \\
&= \gamma^{-1}(\alpha(x) \cdot \alpha(y)^{-1} \cdot \gamma(z) \cdot \beta(u)^{-1} \cdot \beta(v)) \\
&= \gamma^{-1}(\alpha(x) \cdot \beta(y\backslash z) \cdot \beta(u)^{-1} \cdot \beta(v)) \\
&= \gamma^{-1}(\gamma(x * (y\backslash z)) \cdot \beta(u)^{-1} \cdot \beta(v)) \\
&= \gamma^{-1}(\alpha((x * (y\backslash z))/u) \cdot \beta(v)) \\
&= ((x * (y\backslash z))/u) * v.
\end{aligned}$$

Sei nun umgekehrt $(Q, *)$ eine Quasigruppe und es gelte

$$x * (y\backslash((z/u) * v)) = ((x * (y\backslash z))/u) * v.$$

Wir wählen $a, b \in Q$ fest und definieren

$$x *_1 y := (x * (a\backslash b))/y$$

$$x *_2 y := x *_3 y := x * y$$

$$x *_4 y := a\backslash((b/x) * y).$$

Es folgt

$$\begin{aligned}(x *_1 y) *_2 z &= ((x * (a\backslash b))/y) * z \\ &= x * (a\backslash((b/y) * z)) \\ &= x *_3 (y *_4 z).\end{aligned}$$

Erfüllen die Quasigruppen $(Q, *_i)$, $i = 1, 2, 3, 4$ das so genannte verallgemeinerte Assoziativgesetz $(x *_1 y) *_2 z = x *_3 (y *_4 z)$ so sind sie isotop zu einer Gruppe (siehe [18] Theorem 17 oder [1]). Insbesondere ist also $(Q, *)$ isotop zu einer Gruppe. □

Beispiel 3.2 *(Evans [25]) Ein Paar orthogonaler lateinischer Quadrate ist eine Algebra* $(Q, *_1, \backslash_1, /_1, *_2, \backslash_2, /_2, \vee, \wedge)$ *mit acht binären Operationen, so dass gilt*

- $(Q, *_1, \backslash_1, /_1)$ *ist eine Quasigruppe*
- $(Q, *_2, \backslash_2, /_2)$ *ist eine Quasigruppe*
- $(x *_1 y) \wedge (x *_2 y) = x$ *und* $(x \wedge y) *_1 (x \vee y) = x$
- $(x *_1 y) \vee (x *_2 y) = y$ *und* $(x \wedge y) *_2 (x \vee y) = y$.

Damit ist garantiert, dass die Gleichungen $x *_1 y = a$ und $x *_2 y = b$ für alle $a, b \in Q$ eindeutig bestimmte Lösungen $x = a \wedge b$ und $y = a \vee b$ besitzen und damit $(Q, *_1)$ und $(Q, *_2)$ orthogonal zueinander sind.

Andererseits kann ein Paar $(Q, *_1)$, $(Q, *_2)$ orthogonaler lateinischer Quadrate gemäß Definition 3.15 als Algebra $(Q, *_1, \backslash_1, /_1, *_2, \backslash_2, /_2, \vee, \wedge)$ angesehen werden, mit den üblichen Divisionen und mit $x \wedge y := u$, $x \vee y := v$ falls $u, v \in Q$ die eindeutigen Lösungen der Gleichungen $u *_1 v = x$ und $u *_2 v = y$ sind.

Kapitel 4

Konstruktion von Quasigruppen

Beim Versuch, die Eulersche Vermutung zu beweisen oder zu widerlegen, entstand eine Vielzahl von Konstruktionen für Quasigruppen. In diesem Abschnitt stellen wir einen Teil dieser und weiterer Konstruktionen zusammen. Bei der Vielzahl ist es allerdings kaum möglich, alle in der Literatur auftauchenden Konstruktionen aufzulisten. Neben [21], [22] von Denes und Keedwell findet sich eine sehr gute Übersicht im Buch Quasigroups and Loops - Theory and Applications [16]. Diese Konstruktionen werden uns später ermöglichen, die Vermutung von Ecker und Poch zu widerlegen.

4.1 Geometrische Konstruktionen

Historisch gesehen waren die geometrischen Probleme, wie die Koordinatisierung eines Netzes oder einer projektiven Ebene, die Triebfeder für die Untersuchung von Quasigruppen. In diesem Kapitel betrachten wir daher einige Konstruktionen, die durch diese, aber auch durch neuere Fragestellungen entstanden.

Eine *Inzidenzstruktur* ist ein Tripel $(\mathcal{P}, \mathcal{G}, \mathcal{I})$ von Mengen mit $\mathcal{P} \cap \mathcal{G} = \emptyset$ und $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{G}$. Die Elemente von $\mathcal{P}$ bezeichnet man im Allgemeinen als Punkte, die von $\mathcal{G}$ als Geraden (oder auch Blöcke). Ist P inzident zu g, d.h. $(P, g) \in \mathcal{I}$, dann sagen wir, der Punkt P liegt auf der Geraden g oder die Gerade g geht durch den Punkt P. Ist h eine weitere Gerade, die durch P geht, so sagen wir, g und h schneiden sich im Punkt P.

Punkte, die auf einer Geraden liegen, werden kollinear genannt. Geraden, die alle durch einen gemeinsamen Punkt gehen, nennen wir kopunktal.

Definition 4.1 *Eine Inzidenzstruktur heißt* projektive Ebene*, wenn gilt:*

1. *Durch zwei verschiedene Punkte geht genau eine Gerade.*

2. *Zwei verschiedene Geraden schneiden sich in genau einem Punkt.*

3. *Es gibt mindestens vier Punkte, von denen keine drei Punkte kollinear sind.*

Die dritte Eigenschaft wird benötigt, um triviale Fälle auszuschließen. Sie besagt, dass eine projektive Ebene ein Viereck enthalten muss.

Definition 4.2 *Die Geraden einer Inzidenzstruktur seien in k disjunkte Klassen, Parallelklassen genannt, partitioniert. Wir nennen sie* k-Netz*, wenn gilt:*

1. *Jeder Punkt liegt auf genau einer Geraden jeder Klasse.*

2. *Je zwei Geraden von verschiedenen Klassen schneiden sich in genau einem Punkt.*

3. *Es gibt mindestens* 3 *Parallelklassen und jede Gerade besteht aus wenigsten zwei Punkten.*

Die zu einem Punkt P eindeutig bestimmte Gerade der Klasse $\mathcal{G}_i$, auf der P liegt, bezeichnen wir mit $g_i(P)$. Ein k-Netz, in dem je zwei Punkte kollinear sind, heißt affine Ebene.

Mit einem k-Netz kann man k Äquivalenzrelationen auf der Menge $\mathcal{P}$ durch

$$\Theta_i := \{(x, y) \in \mathcal{P}^2 | x \in g_i(y)\}$$

definieren (und umgekehrt), für die für verschiedene i, j gilt

$$\Theta_i \cap \Theta_j = \Delta_{\mathcal{P}} \quad \text{und} \quad \Theta_i \circ \Theta_j = \nabla_{\mathcal{P}}.$$

Aus einer affinen Ebene erhält man eine projektive Ebene, indem man zu jeder Parallelklasse einen Punkt ergänzt. Diese Punkte fassen wir zu einer neuen Geraden zusammen (die Gerade bei Unendlich). Jede Gerade einer Parallelklasse wird um den entsprechenden neu hinzugenommenen Punkt erweitert (die Parallelen schneiden sich gedanklich in einem Punkt bei Unendlich).

Umgekehrt erhalten wir aus einer projektiven Ebene eine affine Ebene, wenn wir eine beliebige Gerade sowie alle zugehörigen Punkte entfernen.

4.1.1 Konstruktion mit einem k-Netz

Liegen auf einer Geraden eines k-Netzes n Punkte, so sieht man leicht, dass dann auch auf allen anderen Geraden n Punkte liegen und jede Klasse aus genau n Geraden besteht. Ebenso gilt, wenn auf einer Geraden einer projektiven Ebene

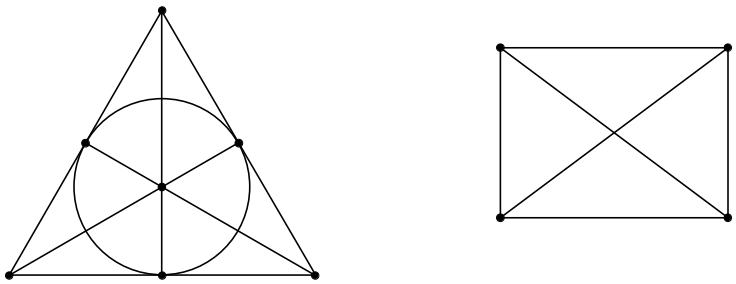

Abbildung 4.1: Projektive und affine Ebene der Ordnung 2

$n+1$ Punkte liegen, so auch auf jeder anderen Geraden, und in jedem Punkt schneiden sich $n+1$ verschiedene Geraden. In diesem Fall sagen wir, das k-Netz bzw. die projektive Ebene hat die Ordnung n.

Wir zeigen nun (vgl. [8]), dass eine enge Verbindung zwischen einem k-Netz und Quasigruppen besteht. Sei ein 3-Netz der Ordnung n mit den Geradenklassen $\mathcal{G}_1, \mathcal{G}_2$ und $\mathcal{G}_3$ gegeben und Q eine Menge mit n Elementen. Wir legen ein $g \in \mathcal{G}_1$ fest. Die Punkte von g benennen wir nach den Elementen von Q, weiterhin sei ein $e \in Q$ fest gewählt. Auf Q definieren wir eine Quasigruppe durch folgende Definition: für $x, y \in Q$ sei P der Schnittpunkt der Geraden $g_2(e)$ und $g_3(y)$. Weiterhin sei R der Schnittpunkt der Geraden $g_1(P)$ und $g_2(x)$ und schließlich z der Schnittpunkt von $g_1(e)$ und $g_3(R)$. Mit $x * y := z$ definiert nun $(Q, *)$ einen Loop (siehe Abbildung).

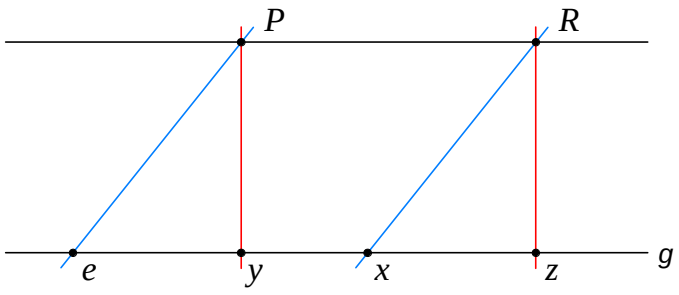

Abbildung 4.2: 3-Netz Konstruktion I

Eine weitere Konstruktion mit einem 3-Netz stammt von Bruck [12]. Die Geraden jeder Klasse werden nach den Elementen von Q benannt. Wir definieren $x * y := z$, wenn die Geraden $g_{1,x} \in \mathcal{G}_1, g_{2,y} \in \mathcal{G}_2$ und $g_{3,z} \in \mathcal{G}_3$ kopunktal sind. Mit

dieser Definition ist $(Q, *)$ eine Quasigruppe.

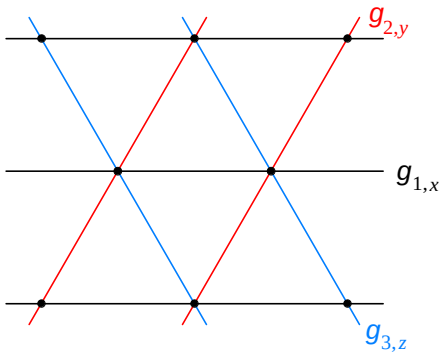

Abbildung 4.3: 3-Netz Konstruktion II

Umgekehrt kann man mit dieser Methode aus einer Quasigruppe ein 3-Netz konstruieren. Die Punktmenge ist $\mathcal{P} := Q \times Q$. Die Geraden sind $g_{1,i} := \{(i, x) | x \in Q\}$, $g_{2,i} := \{(x, i) | x \in Q\}$ und $g_{3,i} := \{(x, y) | i = x * y\}$.

Theorem 4.1 *(vgl. [22], Seite 344) Mit einem k-Netz der Ordnung n lassen sich $k - 2$ paarweise orthogonale lateinische Quadrate der Ordnung n konstruieren. Insbesondere lassen sich $n - 1$ paarweise orthogonale lateinische Quadrate der Ordnung n mit einer projektiven oder affinen Ebene der Ordnung n konstruieren.*

Beweis Zu den Klassen $\mathcal{G}_1$, $\mathcal{G}_2$ und $\mathcal{G}_i$ mit $k \geq i \geq 3$ definieren wir $x *_i y := z$, falls $g_{1,x}, g_{2,y}$ und $g_{i,z}$ kopunktal sind. Um zu zeigen, dass die Quasigruppen $(Q, *_3), \ldots, (Q, *_k)$ paarweise orthogonal sind, nehmen wir $x *_i y = u, x *_j y = v$ und $r *_i s = u, r *_j s = v$ an. Daraus folgt, dass sich die Geraden $g_{1,x}, g_{2,y}, g_{i,u}, g_{j,v}$ und $g_{1,r}, g_{2,s}, g_{i,u}, g_{j,v}$ im selben Punkt schneiden. Dies ist aber nur möglich, wenn $x = r$ und $y = s$ gilt.

4.1.2 Konstruktion mit einer projektiven Ebene

Quasigruppen können wir auch durch Koordinatisierung einer projektiven Ebene erhalten (siehe Hall [30]). Sei π eine projektive Ebene der Ordnung n, A und B zwei feste Punkte von π und g die Gerade durch A und B. Wir setzen $\pi' = \pi \setminus g$, d.h. π' ist die affine Ebene, die wir erhalten, wenn wir g und alle Punkte von g aus π entfernen. Sei $Q = \{0, \ldots, n - 1\}$ eine Menge mit n Elementen. Wir benennen die A-Geraden (d.h. die Geraden, die durch A gehen, außer g) beliebig mit den Elementen von Q und analog die B-Geraden. Jeder Punkt von π' liegt nun auf

einer eindeutig bestimmten A- bzw. B-Geraden, so dass wir ihm eine Koordinate $(x, y) \in Q \times Q$ zuordnen können. Nun sei O der Punkt $(0, 0)$, I der Punkt $(1, 1)$ und E der Schnittpunkt der Geraden g und der Geraden g' durch I und O.

Auf Q definieren wir nun eine dreistellige Verknüpfung T wie folgt: für $r, u, v \in Q$ sei M der Punkt auf g, der auch auf der Geraden durch $(0, 0)$ und $(1, u)$ liegt. Weiterhin sei (r, s) der Schnittpunkt der Geraden die durch M und $(0, v)$ geht und der A-Geraden mit der Bezeichnung a_r, dann sei

$$T(r, u, v) := s$$

und (Q, T) heißt Ternärkörper oder auch Ternärring.

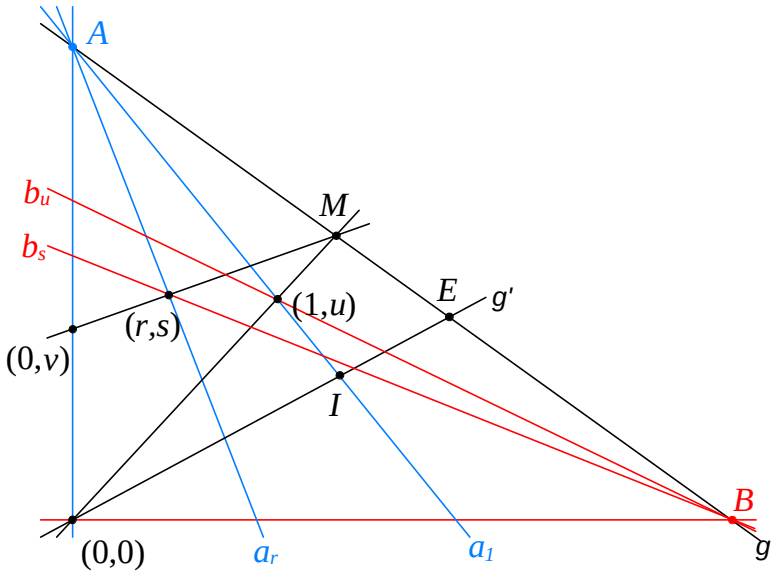

Abbildung 4.4: Konstruktion mit einer projektiven Ebene

Nun definieren wir zwei binäre Verknüpfungen $+$ auf Q und $\cdot$ auf $Q^* = Q \setminus \{0\}$ durch

$$x + y := T(x, 1, y) \quad \text{und} \quad x \cdot y = T(x, y, 0),$$

dann sind $(Q, +)$ und $(Q^*, \cdot)$ Quasigruppen (sogar Loops durch geeignete Benennung der B-Geraden). Die Konstruktion wird klarer, wenn wir an die kartesischen Koordinaten der Ebene denken. Dann ist g die Gerade bei Unendlich, die A-Geraden sind vertikal und die B-Geraden horizontal. Die Gerade durch O und B ist die x-Achse und die Gerade durch O und A die y-Achse. Die Gerade g' ist die Gerade $y = x$ und

$$T(r, u, v) = ru + v.$$

In diesem Fall sind + und · die übliche Addition und Multiplikation und (Q, T) heißt linearer Ternärkörper.

4.1.3 Mittelpunkt-Konstruktion

Sei Q die Menge der Punkte eines euklidschen Raumes. Definiere $*$ auf Q durch $z := x * y$, wobei z der Mittelpunkt von x und y ist. Dann ist $(Q, *)$ eine kommutative distributive Quasigruppe (siehe [60], [62]).

Auch ohne eine metrische Struktur kann man einen Mittelpunkt definieren [26]: Sei Q die Menge der Eckpunkte eines n-Ecks, n ungerade. Für $x, y \in Q$ betrachten wir den Weg mit einer ungeraden Anzahl Eckpunkten. Setze $x * y$ gleich den Eckpunkt, der in der Mitte dieses Weges liegt.

Sei Q die Menge der Punkte einer Inzidenzstruktur, bei der jede Gerade aus einer ungeraden Anzahl Punkten besteht und bei der durch zwei verschiedene Punkte genau eine Gerade geht. Für $x, y \in Q$ sei g die Gerade durch x und y und $x * y$ der Mittelpunkt im obigen Sinne. Dabei nehmen wir an, g sei ein n-Eck (ggf. geschlossen in der Unendlichkeit).

Sei Q die Menge der Punkte einer Parabel der euklidschen Ebene. Es sei (vgl. [45])

$$x * x := x$$

und für verschiedene $x, y \in Q$

$$x * y := z,$$

wobei z der Punkt ist, bei dem die Tangente durch z parallel zu der Geraden durch x und y ist (siehe Abbildung 4.5).

In allen Fällen ist $(Q, *)$ eine kommutative Quasigruppe.

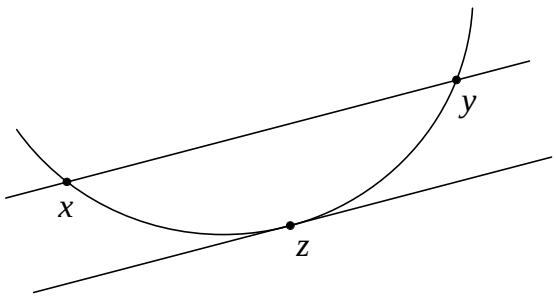

Abbildung 4.5: Mittelpunkt bei einer Parabel

Eine Verallgemeinerung der Konstruktion mit einer Parabel erhalten wir wie folgt [62]. Sei C ein Kegelschnitt und g eine feste Tangente an C. Sei Q die Menge

der Punkte von C, mit Ausnahme des Punktes, der g berührt. Definiere $x * x = x$ und $z := x * y$ (x, y, z paarweise verschieden) so, dass die Tangente an x sich mit der Geraden durch z und y auf g schneidet. Dann ist $(Q, *)$ eine idempotente Quasigruppe.

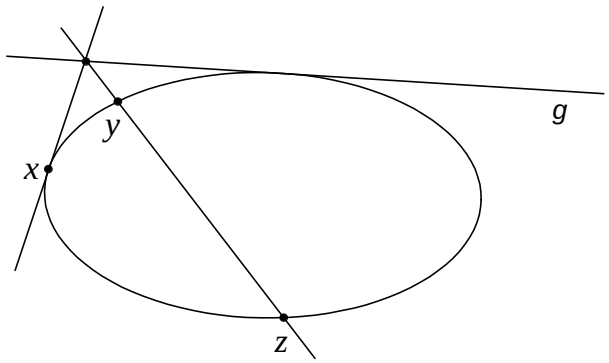

Abbildung 4.6: Kegelschnittkonstruktion

4.2 Konstruktionen basierend auf Designs

In diesem Abschnitt untersuchen wir Konstruktionen, die auf einem Design basierend in einer Quasigruppe bzw. einem Loop resultieren.

Ein Design ist eine endliche Inzidenzstruktur $(\mathcal{P}, \mathcal{B}, \in)$, wobei $\mathcal{B}$ Teilmenge der Potenzmenge von $\mathcal{P}$ ist. Die Elemente von $\mathcal{B}$ nennt man Blöcke, wobei jeder Block aus mindestens 2 Elementen besteht. Zwei wichtige Designs sind die Blockpläne, auch BIBDs (balanced incomplete block designs) genannt, und die PBDs (pairwise balanced designs).

In einem $S_\lambda(t, k, v)$ Blockplan, $v = |\mathcal{P}|$, haben alle Blöcke die Größe k und t verschieden Punkte liegen in genau λ Blöcken.

Sei $K \subset \mathbb{N}$ eine Menge (die Menge der Blocklängen). Wir nennen ein PBD ein $S_\lambda(2, K, v)$ wenn je zwei verschiedene Punkte in genau λ Blöcken liegen und die Blöcke eine Größe aus der Menge K haben. Ist $\lambda = 1$ so schreiben wir kurz $S(2, K, v)$.

Beispiel Mit dieser Terminologie ist eine projektive Ebene der Ordnung n ein $S(2, n+1, n^2+n+1)$ und die affine Ebene ein $S(2, n, n^2)$.

Beispiel Für $v = 10$ und $K = \{3, 4\}$ definieren wir die Blöcke durch

$$\begin{array}{lll} B_1 = \{1,2,3,7\} & B_2 = \{4,5,6,7\} & B_3 = \{8,9,10,7\} \\ B_4 = \{1,4,8\} & B_5 = \{2,5,9\} & B_6 = \{3,6,10\} \\ B_7 = \{1,5,10\} & B_8 = \{3,5,8\} & B_9 = \{3,4,9\} \\ B_{10} = \{2,4,10\} & B_{11} = \{1,6,9\} & B_{12} = \{2,6,8\} \end{array}$$

Damit erhalten wir ein $S(2, \{3, 4\}, 10)$.

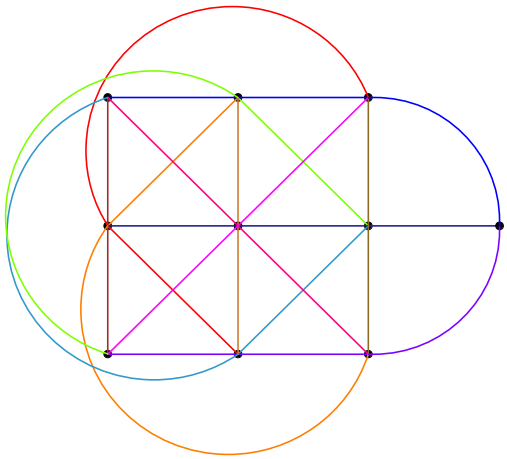

Abbildung 4.7: $S(2, \{3, 4\}, 10)$ Design

4.2.1 Steiner-Quasigruppen und Steinertripelsysteme

Einen $S(2, 3, v)$ Blockplan nennt man ein Steinertripelsystem (kurz STS). Es ist nach Jacob Steiner benannt, der sich mit deren Existenz beschäftigte. In einer 1853 erschienenen Aufgabe [63] stellte er die Frage:

> *Welche Zahl N von Elementen hat die Eigenschaft, dass sich die Elemente so zu dreien ordnen lassen, dass je zwei in einer, aber nur einer Verbindung vorkommen?*

Die Aufgabe hatte allerdings bereits Kirkman [35] im Jahre 1847 gelöst:

Theorem 4.2 *Sei v eine natürliche Zahl mit $v > 3$. Genau dann existiert ein Steinertripelsystem mit v Punkten, wenn $v \equiv 1 \mod 6$ oder $v \equiv 3 \mod 6$ ist.*

Mit Hilfe eines Steinertripelsystems erhalten wir eine idempotente total symmetrische (Steiner-)Quasigruppe auf folgende Weise: sei Q die Punktmenge des STS's, definiere $*$ auf Q durch

$$x * x = x, \qquad x * y = z,$$

wobei x und y verschiedene Elemente von Q sind und $\{x, y, z\}$ der eindeutig bestimmte Block ist, der x und y enthält.

Umgekehrt erhält man ein STS aus einer Steiner-Quasigruppe, indem man die Blöcke definiert durch $\{x, y, z\}$, wobei $x * y = z$ (x, y, z paarweise verschieden). Offensichtlich besteht also eine Eins-zu-Eins-Beziehung zwischen Steinertripelsystemen und Steiner-Quasigruppen.

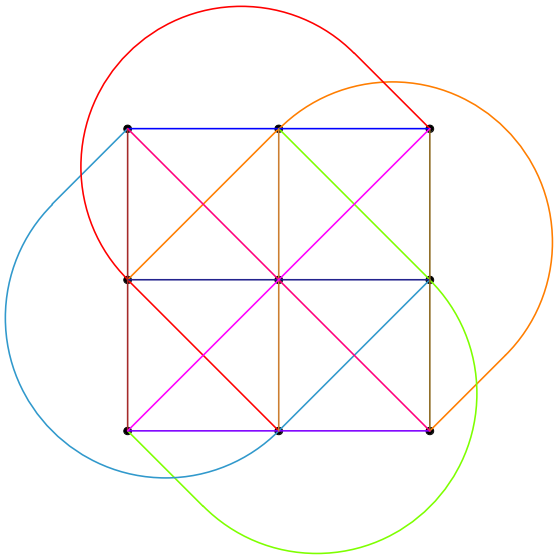

Abbildung 4.8: Steinertripelsystem mit 9 Punkten

Von Netto [46] stammen folgende Konstruktionen. Wenn $p = 6m + 1$ eine Primzahl ist und g eine primitive Wurzel modulo p, dann definieren wir die Blöcke durch $\{x, x + g^y, x + g^{m+y}\}$, wobei $0 \leq x < p$, $0 \leq y < m$ und die Rechnung Modulo p erfolgt. Dies definiert ein STS der Ordnung p.

Sei $p = 6m + 5$ eine Primzahl und g eine primitve Wurzel Modulo p. Wir betrachten die Tripel $\{x, x + g^y, x + g^{y+3m+2}\}$ für $0 \leq x < 3p$ und $0 \leq y < 3m + 2$ zusammen mit den Tripeln der Form $\{x, x+p, x+2p\}$ für $0 \leq x < p$ mit Rechnung Modulo $3p$. Dies definiert ein STS der Ordnung $3p$.

Gegeben sei ein STS der Ordnung n auf der Menge $\{1, \ldots, n\}$. Wir definieren ein STS der Ordnung $2n+1$ auf $\{0, \ldots, 2n\}$ durch die Tripel $\{0, x, x+n\}$,$1 \leq x \leq n$,

sowie $\{x, y, z\}$, $\{x, y+n, z+n\}$, $\{x+n, y, z+n\}$ und $\{x+n, y+n, z\}$, wobei $\{x, y, z\}$ ein Tripel aus dem gegebenen STS ist.

Ebenfalls von Netto stammt die Aussage, dass das Kreuzprodukt zweier STSe der Ordnung n und m ein STS der Ordnung $n \cdot m$ ergibt.

4.2.2 PBD- und GDD-Konstruktionen

Eine Konstruktion von Wilson [69] nutzt ein PBD, um eine Quasigruppe zu definieren. Dazu sei ein PBD auf der Menge Q gegeben und zu jedem Block B sei $(B, *_B)$ eine idempotente Quasigruppe. Auf Q definieren wir $*$ durch

$$x * x = x, \qquad x * y = x *_B y$$

für $x \neq y$, wobei B der eindeutig bestimmte Block ist, der x und y enthält. Dann ist $(Q, *)$ eine idempotente Quasigruppe.

Eine Verallgemeinerung dieser Konstruktion erhält man durch ein GDD (group divisible design). Sei $\mathcal{D} = (\mathcal{P}, \mathcal{G} \cup \mathcal{B}, \in)$ ein Design, wobei $\mathcal{G}$ eine Partition der Punktmenge $\mathcal{P}$ darstellt und zu zwei verschiedenen Punkten entweder genau eine Punktklasse (auch „Gruppe“ genannt) $G \in \mathcal{G}$ oder genau ein Block $B \in \mathcal{B}$ existiert, der diese Punkte enthält, dann nennen wir $\mathcal{D}$ ein GDD. Es sei zu jeder Punktklasse G eine Quasigruppe $(G, \circ_G)$ und zu jedem Block B eine idempotente Quasigruppe $(B, *_B)$ gegeben. Wir definieren eine Quasigruppe $(\mathcal{P}, *)$ auf der Punktmenge des GDD durch

$$x * y = x \circ_G y, \qquad x * z = x *_B z,$$

falls x und y (nicht zwingend verschieden) in der selben Punktklasse G liegen und x, z verschiedene Elemente des Blocks B sind.

Diese Konstruktionen werden zur rekursiven Konstruktion von paarweise orthogonalen lateinischen Quadraten bzw. von selbstorthogonalen Quasigruppen herangezogen. Außerdem eignen sie sich dazu, Quasigruppen zu konstruieren, welche vorgegebene Quasigruppen als Unterquasigruppen enthalten.

4.3 Algebraische und kombinatorische Konstruktionen

Nun betrachten wir einige algebraische und kombinatorische Konstruktionsmöglichkeiten von Quasigruppen. Diese ergeben sich zum Teil direkt aus den Definitionen aus Kapitel 3.

4.3.1 Produktbildung

Die wohl bekannteste Möglichkeit, aus gegebenen Algebren neue zu konstruieren, ist die Bildung des direkten Produktes. Hat man z.B. zwei Quasigruppen $(N, \cdot)$ und $(Q, *)$, so ist das direkte Produkt $(N \times Q, \otimes)$ dieser Quasigruppen definiert durch

$$(n, q) \otimes (m, r) = (n \cdot m, q * r).$$

Dieser einfache Ansatz lässt sich auf vielfache Weise verallgemeinern. Ein erster Schritt dazu ist das semi-direkte Produkt: seien $(N, \cdot)$, $(Q, *)$ Quasigruppen und $f_{q,r}$ Permutationen der Menge N, $q, r \in Q$, dann definieren wir die Multiplikation $\otimes$ auf $N \times Q$ durch

$$(n, q) \otimes (m, r) = (f_{q,r}(n \cdot m), q * r).$$

Ein etwas allgemeinerer Ansatz stammt von Bruck [13]. Wir definieren $\otimes$ durch

$$(n, q) \otimes (m, r) = (n \bigtriangledown_{q,r} m, q * r),$$

wobei $(N, \bigtriangledown_{q,r})$ eine Quasigruppe für alle $q, r \in Q$ ist. Von Wilson [68] wurde diese Konstruktion das quasi-direkte Produkt von N und Q mit den lokalen Operatoren $\bigtriangledown_{q,r}$ genannt. Eine Quasigruppe der Ordnung $n = mp$ die durch das quasi-direkte Produkt der Quasigruppen $(N, \bigtriangledown_{q,r})$ der Ordnung p und $(\mathbb{Z}_m, +)$ entstanden ist, nennen wir *Quasigruppe vom p-Stufen Typ.*

Ein Ansatz von Johnson und Sharma [34], die $\bigtriangledown_{q,r}$ zu definieren, lautet wie folgt: für alle $q, r \in Q$ seien $\alpha_{q,r}$ und $\beta_{q,r}$ Permutationen von N und $\gamma_{q,r}$ eine Permutation von $N \times N$. Wir definieren $\bigtriangledown_{q,r}$ durch

$$n \bigtriangledown_{q,r} m = \sigma(\gamma_{q,r}(\alpha_{q,r}(m), \beta_{q,r}(n))),$$

wobei $\sigma(n, m) = n \cdot m$ die Operation auf N ist.

Bisher haben wir das Produkt von zwei Quasigruppen N und Q benutzt, um eine Erweiterung von N durch Q zu konstruieren. Diese Konstruktionen ergeben, eingeschränkt auf die zweite Koordinate, wieder die Quasigruppe Q. Im folgenden betrachten wir ein Produkt bei dem weder die erste noch die zweite Koordinate die gleiche Multiplikation wie die ursprüngliche Quasigruppe besitzen.

Das verallgemeinerte semi-direkte Produkt wurde von Baker [2] eingeführt. Dazu seien $(Q, +_1), \ldots, (Q, +_m)$ idempotente Quasigruppen auf der Menge Q. Weiterhin seien $(S, \bigtriangledown_1)$ und $(S, \bigtriangledown_2)$ Quasigruppen und $\Theta : S \times S \to \{1, \ldots, m\}$ eine Abbildung. Wir definieren die Quasigruppe $(Q \times S, \otimes)$ durch

$$(x, s) \otimes (y, t) = (x +_{\Theta(s,t)} y, s \bigtriangledown_1 t), \text{ falls } x \neq y$$

$$(x, s) \otimes (x, t) = (x, s \bigtriangledown_2 t).$$

Falls $\bigtriangledown_1 = \bigtriangledown_2$ ist, so entspricht das verallgemeinerte semi-direkte Produkt dem quasi-direkten Produkt.

4.3.2 Isotopie

Während wir im vorhergehenden Abschnitt eine Quasigruppe auf einer neuen Grundmenge definiert haben, so betrachten wir jetzt die Möglichkeit, auf einem vorgegebenen algebraischen System eine neue Operation zu definieren. Bei Quasigruppen bietet es sich an, die Isotopien zu betrachten. Als Ausgangspunkt kann eine Gruppe, als Spezialfall einer Quasigruppe, dienen. Ein einfaches Beispiel für die Gruppe $(\mathbb{Z}_n, +)$ ist, eine Quasigruppe $(\mathbb{Z}_n, *)$ durch

$$x * y = -x + y$$

zu definieren. Im Ring $(\mathbb{Z}_n, +, \cdot)$ ist die Abbildung $\alpha_a : x \mapsto a \cdot x$ genau dann eine Permutation, wenn a relativ prim zu n ist, also $ggT(a, n) = 1$. Sind a und b relativ prim zu n, so ist

$$x * y = \alpha_a(x) + \alpha_b(y) = ax + by$$

eine Quasigruppe. Sind außerdem noch $a + b$ und $a - b$ relativ prim zu n, so ist $(\mathbb{Z}_n, *)$ selbst-orthogonal (Sade [56]).

Stein [62] untersuchte die Existenz von distributiven Quasigruppen (siehe Definition 3.17). Sind r und s relativ prim zu n, n ungerade, und $r + s =_n 1$, so ist $(\mathbb{Z}_n, *)$ mit $x * y = rx + sy$ eine distributive Quasigruppe. Mit der Wahl $s = 1 - r$ und $r \neq 0, 1$ ist $(\mathrm{GF}(2^n), *)$ eine distributive Quasigruppe. Mit Hilfe des direkten Produkts konnte Stein damit distributive Quasigruppen für alle Ordnungen $n \equiv 0, 1, 3 \mod 4$ konstruieren. Außerdem zeigte er, dass es keine distributiven Quasigruppen der Ordnung $4k + 2$ gibt.

In einer Gruppe $(G, \cdot)$ mit ungerader Ordnung ist die Abbildung $\sigma : x \mapsto x^2$ eine Permutation (Bruck [14]). Mit der Definition

$$x * y = \sigma^{-1}(x \cdot y)$$

ist $(G, *)$ eine idempotente Quasigruppe. Schreibt man G additiv, so ist $x * y = (x + y)/2$.

Eine weitere Konstruktion von Bruck [14] zeigt, dass es im Gegensatz zu Gruppen eine Quasigruppe ohne echte Unterquasigruppen gibt: dazu sei eine idempotente Quasigruppe $(Q, \cdot)$ mit $Q = \{1, \ldots, n\}$ gegeben. Weiterhin sei $\sigma = (1\ \ 2\ \ \ldots\ \ n)$ der Zykel, der i auf $i + 1$ $(i < n)$ und n auf 1 abbildet. Die Quasigruppe

$$x * y = \sigma(x \cdot y)$$

hat dann keine echte Unterquasigruppe, denn ist i in einer Unterquasigruppe enthalten, dann auch $i * i = \sigma(i \cdot i) = \sigma(i)$. Induktiv erhält man somit alle Elemente von Q.

4.3.3 Parastrophien

Zu einer Quasigruppe $(Q, \cdot)$ können wir folgende sechs neue Operationen definieren (vergleiche Abschnitt 3.2):

$$\begin{aligned}
x *_1 y &= x \cdot y \\
x *_2 y &= z, \qquad \text{wobei } z \text{ die Lösung von } x \cdot z = y \text{ ist} \\
x *_3 y &= z, \qquad \text{wobei } z \text{ die Lösung von } z \cdot x = y \text{ ist} \\
x *_4 y &= y *_1 x \\
x *_5 y &= y *_2 x \\
x *_6 y &= y *_3 x
\end{aligned}$$

Von Sade [55] wurden je zwei dieser Quasigruppen parastrophisch genannt und die einzelnen Quasigruppen heißen Parastrophien voneinander. In der Literatur taucht außerdem der Begriff *konjugierte Quasigruppen* für diese Quasigruppen auf. Ist $(Q, *)$ symmetrisch, dann ist $*_4 = *_1$, $*_3 = *_2$ und $*_6 = *_5$. Ist $(Q, *)$ total symmetrisch (siehe Definition 3.16), so sind alle sechs Operationen gleich.

4.3.4 Diagonalmethode

Von Sade [54] stammt folgende Konstruktionsmethode, die so genannte Diagonalmethode. Auf $(\mathbb{Z}_n, +)$ sei p eine Permutation der Menge $\mathbb{Z}_n$, so dass auch $x \mapsto x - p(x)$ eine Permutation ist. Wir definieren $*$ durch

$$x * y = p(x - y) + y,$$

dann ist $(\mathbb{Z}_n, *)$ eine Quasigruppe und jede Translation $\sigma_h : x \mapsto x + h$ ist ein Automorphismus.

Falls p eine solche Permutation ist, so auch die folgenden Permutationen

$$\begin{aligned} & \varphi(x) = x - p(x), \\ & \varphi(x) = p^{-1}(x), \\ & \varphi(x) = -p(-x), \\ & \varphi(x) = x + p(-x), \\ & \varphi(x) = p(x) + h \\ \text{und} \quad & \varphi(x) = p(x + h) \end{aligned}$$

für beliebige h. Sind a und $a - 1$ relativ prim zu n, so erfüllt $p(x) = ax + b$ die gewünschte Bedingung.

Falls p auf $\mathbb{Z}_n$ und $\pi_0, \ldots, \pi_{n-1}$ auf $\mathbb{Z}_m$ die Bedingung erfüllen, so auch φ auf $\mathbb{Z}_{mn}$ mit

$$\varphi(x) = p(r) + n\pi_r(s)$$

für $x = ns + r$.

Beispiel Sei $(\mathbb{Z}_7, *)$ definiert durch $x * y := 2(x - y) + y = 2x - y$. Dann erhalten wir

$*$	0	1	2	3	4	5	6
0	0	6	5	4	3	2	1
1	2	1	0	6	5	4	3
2	4	3	2	1	0	6	5
3	6	5	4	3	2	1	0
4	1	0	6	5	4	3	2
5	3	2	1	0	6	5	4
6	5	4	3	2	1	0	6

Wie wir sehen, besitzen Quasigruppen, die mit der Diagonalmethode erzeugt wurden, eine Zerlegung in disjunkte Transversalen und damit ein orthogonales Komplement. Eine zu $(\mathbb{Z}_7, *)$ orthogonale Quasigruppe lässt sich leicht angeben:

·	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	6	0	1	2	3	4	5
2	5	6	0	1	2	3	4
3	4	5	6	0	1	2	3
4	3	4	5	6	0	1	2
5	2	3	4	5	6	0	1
6	1	2	3	4	5	6	0

4.3.5 Verallgemeinertes singulär direktes Produkt

Von Sade [56] und Lindner [38], [39] wurde das (verallgemeinerte) singulär direkte Produkt eingeführt. Damit konnten neue Steiner-Quasigruppen bzw. selbstorthogonale Quasigruppen konstruiert werden.

Es sei $(Q, *)$ eine Quasigruppe mit einer Unterquasigruppe $(S, *)$ und $(V, \bigtriangledown)$ eine idempotente Quasigruppe. Weiterhin sei $P = Q \backslash S$ und $(P, \otimes_{v,w})$ eine Quasigruppe für alle geordneten Paare $(v, w) \in V \times V$ mit verschiedenen Elementen v und w.

Auf der Menge $S \cup (P \times V)$ definieren wir das *verallgemeinerte singulär direkte Produkt* $\cdot$ durch

$$\begin{aligned}
x \cdot y &= x * y \\
x \cdot (r, v) &= (x * r, v) \\
(r, v) \cdot y &= (r * y, v) \\
(r, v) \cdot (s, v) &= r * s, \text{ falls } r * s \in S \\
(r, v) \cdot (s, v) &= (r * s, v), \text{ falls } r * s \in P \\
(r, v) \cdot (s, w) &= (r \otimes_{v,w} s, v \bigtriangledown w), \text{ falls } v \neq w,
\end{aligned}$$

wobei $x, y \in S$, $r, s \in P$ und $v, w \in V$.

Ist $\otimes_{v,w}$ für alle $v, w \in V$, $v \neq w$, die gleiche Operation, so haben wir das singulär direkte Produkt von Sade und falls außerdem noch $S = \emptyset$ und $\otimes_{v,w} = *$ gilt, so handelt es sich um das übliche direkte Produkt.

Eine weitere Verallgemeinerung von Lindner [40] nimmt statt der Operation $*$ eine Operation $*_v$ für jedes Element $v \in V$ an, die auf der Menge S übereinstimmen. Außerdem muss $(S, *_v)$ eine Unterquasigruppe von $(Q, *_v)$ sein.

Beispiel Sei $Q := \{0,1,2,3\}$, $S := \{0\}$, $r \otimes_{v,w} s := (-r - s + 2v + w - 1)_3 + 1$ und $(Q, *)$, (V, ∇) definiert durch

$*$	0	1	2	3
0	0	1	2	3
1	2	3	0	1
2	3	2	1	0
3	1	0	3	2

∇	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

dann erhalten wir mit dem verallgemeinerten singulär direkten Produkt die Quasigruppe von Abbildung 4.9.

$\cdot$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	2	3	0	1	8	7	9	6	5	4
2	3	2	1	0	7	9	8	5	4	6
3	1	0	3	2	9	8	7	4	6	5
4	5	9	8	7	6	0	4	2	1	3
5	6	8	7	9	5	4	0	1	3	2
6	4	7	9	8	0	6	5	3	2	1
7	8	5	4	6	3	2	1	9	0	7
8	9	4	6	5	2	1	3	8	7	0
9	7	6	5	4	1	3	2	0	9	8

Abbildung 4.9: Verallgemeinertes singulär direktes Produkt

Pelling und Rogers [51] definieren ein singulär direktes Produkt für n Faktoren. Dazu seien $(Q_i, *_i)$, $i = 1, \ldots, n$, disjunkte Quasigruppen mit einer (ggf. trivialen) Unterquasigruppe $(S_i, *_i)$. Wir definieren $P_i = Q_i \setminus S_i$, $S = S_1 \cup \ldots \cup S_n$ und $P = P_1 \times \ldots \times P_n$. $(S, *)$ sei eine Quasigruppe, die auf den S_i mit $*_i$ übereinstimmt, und die $(Q_i, *_i)$ seien idempotent für $i > 1$. Außerdem sei $(P_i, \otimes_i)$ eine idempotente Quasigruppe für alle i. Auf $S \cup P$ definieren wir $\cdot$ durch

$$
\begin{aligned}
x \cdot y &= x * y \\
x_i \cdot (p_1, \ldots, p_n) &= (p_1, \ldots, p_{i-1}, x_i *_i p_i, p_{i+1}, \ldots, p_n) \\
(p_1, \ldots, p_n) \cdot x_i &= (p_1, \ldots, p_{i-1}, p_i *_i x_i, p_{i+1}, \ldots, p_n) \\
(p_1, \ldots, p_n) \cdot (p_1, \ldots, p_n) &= p_1 *_1 p_1 \quad \text{falls } p_1 *_1 p_1 \in S_1 \\
(p_1, \ldots, p_n) \cdot (p_1, \ldots, p_n) &= (p_1 *_1 p_1, p_2, \ldots, p_n) \quad \text{sonst} \\
(p_1, \ldots, p_n) \cdot (p_1, \ldots, p_{i-1}, q_i, p_{i+1}, \ldots, p_n) &= p_i *_i q_i \quad \text{falls } p_i \neq q_i \text{ und } p_i *_i q_i \in S_i \\
(p_1, \ldots, p_n) \cdot (p_1, \ldots, p_{i-1}, q_i, p_{i+1}, \ldots, p_n) &= (p_1, \ldots, p_{i-1}, p_i *_i q_i, p_{i+1}, \ldots, p_n) \\
&\quad \text{falls } p_i \neq q_i \text{ und } p_i *_i q_i \notin S_i \\
(p_1, \ldots, p_n) \cdot (q_1, \ldots, q_n) &= (p_1 \otimes_1 q_1, \ldots, p_n \otimes_n q_n) \quad \text{sonst,}
\end{aligned}
$$

wobei $x, y \in S$, $x_i \in S_i$, $p_i, q_i \in P_i$, dann ist $(S \cup P, \cdot)$ eine Quasigruppe.

4.3.6 Prolongation und Kontraktion

Besitzt eine Quasigruppe eine Transversale, so können wir die *Prolongation*, auch *Insertion-Konstruktion* genannt, durchführen (Osborn [47], Bruck [14]). Eine Transversale ist eine Menge von n Zellen der Verknüpfungstafel einer Quasigruppe der Ordnung n, aus jeder Zeile und Spalte eine Zelle, so dass jedes Element von Q genau einmal in diesen Zellen enthalten ist. Wir können nun eine Quasigruppe der Ordnung $n+1$ konstruieren, indem wir ein weiteres Element u zur Menge Q hinzufügen. Die Verknüpfungstafel der ursprünglichen Quasigruppe erweitern wir um eine Zeile und eine Spalte am rechten bzw. unteren Rand. Ohne die Reihenfolge der Elemente zu ändern, verschieben wir die Zellen der Transversale in diese Zeile und Spalte. Die freiwerdenden Zellen der Transversale sowie die freie Zelle in der rechten unteren Ecke werden mit u gefüllt. Die so konstruierte Verknüpfungstafel ist eine Quasigruppe der Ordnung $n+1$.

$*$	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

$\rightarrow$

$\cdot$	0	1	2	3	4	5
0	5	1	2	3	4	0
1	4	0	1	5	3	2
2	3	5	0	1	2	4
3	2	3	4	0	5	1
4	1	2	5	4	0	3
5	0	4	3	2	1	5

Die Konstruktion kann man auch algebraisch ausdrücken. Sei $(Q, *)$, $Q = \{0, 1, \ldots, n-1\}$, eine Quasigruppe der Ordnung n mit der Transversalen $T =$

(α, β). Wir definieren auf der Menge $Q' = \{0, \ldots, n-1, n\}$ eine Quasigruppe $(Q', \cdot)$ der Ordnung $n+1$ durch:

$$x \cdot y := \begin{cases} n & x, y < n \text{ und } (x, y) \in T \\ x * y & x, y < n \text{ und } (x, y) \notin T \\ x * y' & x < n, y = n \text{ und } (x, y') \in T \\ x' * y & x = n, y < n \text{ und } (x', y) \in T \\ n & x = y = n. \end{cases}$$

Falls Q zwei disjunkte Transversalen besitzt, so kann man diese Konstruktion zweimal anwenden und man erhält eine Quasigruppe der Ordnung $n+2$. Allgemeiner gilt, wenn $(Q, *)$ k disjunkte Transversalen besitzt, so kann man mit wiederholter Prolongation eine Quasigruppe der Ordnung $n+k$ konstruieren.

Von Yamamoto [70] stammt eine leichte Abwandlung. Anstatt die Prolongation mehrfach nacheinander anzuwenden, führt er die Konstruktion in einem Schritt auf folgende Weise durch. Sei Q eine Quasigruppe mit k disjunkten Transversalen, $u_1, \ldots, u_k$ Elemente, die nicht in Q enthalten sind, und $(S, \cdot)$ eine beliebige Quasigruppe auf der Menge $S = \{u_1, \ldots, u_k\}$.

Zwei Permutationen p, q der Menge $\{1, \ldots, k\}$ legen fest, wie die Transversalen am rechten bzw. unteren Rand angeordnet werden: die i-te Transversale wird in der $(n-1+p(i))$-ten Spalte und der $(n-1+q(i))$-ten Zeile in ihrer ursprünglichen Reihenfolge in die $(n+k) \times (n+k)$-große Verknüpfungstafel eingefügt. Die ersten n Zeilen und Spalten der neuen Verknüpfungstafel entsprechen der von Q, wobei die Zellen der i-ten Transversale mit u_i gefüllt werden. In die noch $k \times k$ freien Zellen rechts unten wird die Verknüpfungstafel von $(S, \cdot)$ eingefügt. Damit haben wir eine Quasigruppe der Ordnung $n+k$ konstruiert.

Beispiel Es seien $(Q, *)$ und $(S, \cdot)$ mit $Q = \{0, \ldots, 6\}$ und $S = \{7, 8, 9\}$ wie folgt gegeben:

$*$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	5	6	0	1	2	3	4
2	1	2	3	4	5	6	0
3	2	3	4	5	6	0	1
4	4	5	6	0	1	2	3
5	6	0	1	2	3	4	5
6	3	4	5	6	0	1	2

bzw.

$\cdot$	7	8	9
7	7	8	9
8	9	7	8
9	8	9	7

Wir führen die Konstruktion mit den drei farblich hinterlegten Transversalen von $(Q, *)$ durch. Mit der Wahl $p = (1, 2, 0)$ und $q = (2, 0, 1)$ erhalten wir die Quasigruppe $(Q \cup S, *')$:

$*'$	0	1	2	3	4	5	6	7	8	9
0	7	9	2	3	4	5	8	1	6	0
1	8	7	9	1	2	3	4	0	5	6
2	1	8	7	9	5	6	0	4	2	3
3	2	3	8	7	9	0	1	6	4	5
4	4	5	6	8	7	9	3	2	0	1
5	6	0	1	2	8	7	9	5	3	4
6	9	4	5	6	0	8	7	3	1	2
7	5	2	4	0	3	1	6	7	8	9
8	0	6	3	5	1	4	2	9	7	8
9	3	1	0	4	6	2	5	8	9	7

Die Umkehrung der Prolongation nennt man Kontraktion oder Deletion. Sei z.B. $(Q, *)$, $Q = \{0, 1, \ldots, n\}$ eine Quasigruppe der Ordnung $n + 1$ und es gelte $x * x = n$ und $x * n = n * x$. Wir erhalten eine Quasigruppe der Ordnung n, indem wir die Elemente der letzten Zeile in der Diagonalen anordnen und die n-te Zeile und Spalte entfernen. Die durch die Kontraktion entstehende Quasigruppe $(Q', \cdot)$ mit $Q' = \{0, \ldots, n - 1\}$ lässt sich wie folgt definieren:

$$x \cdot y := \begin{cases} x * y & \text{falls } x \neq y \\ x * n & \text{falls } x = y. \end{cases}$$

Auch hier ist eine Verallgemeinerung möglich. Statt der n-ten Zeile und Spalte entfernt man die a-te Zeile und die b-te Spalte, falls $a * x = x * b$ für alle $x \in Q$ und $a * b = n$ gilt.

4.4 Das Ende der Euler Vermutung

Als Anwendung der bisher aufgeführten Konstruktionen skizzieren wir im folgenden einen Beweis, der die Vermutung von Euler widerlegt. Euler untersuchte um 1779 das Problem der 36 Offiziere.

> *Ist es möglich, 36 Offiziere mit 6 unterschiedlichen Rängen und aus 6 unterschiedlichen Regimenten, so in einem* 6×6 *Quadrat anzuordnen, so dass in einer Reihe bzw. Spalte jeweils genau ein Offizier jeden Ranges und Regiments steht?*

Das Problem ist gleichbedeutend mit der Existenz eines Paares orthogonaler lateinischer Quadrate der Ordnung 6. Euler konnte keine Lösung finden, auch nicht für die Ordnungen 10, 14, usw. Daher vermutete er, dass es kein Paar orthogonaler lateinischer Quadrate der Ordnung $4k+2$ gibt. Im Jahre 1900 zeigte Gaston Tarry [65] durch eine aufwendige Untersuchung aller möglichen Fälle, dass für die Ordnung 6 die Vermutung richtig ist. Erst 1958 bzw. 1959 gelang es Bose, Shrikhande und Parker [9] Gegenbeispiele zu konstruieren und 1960 konnten sie die Vermutung von Euler vollständig widerlegen (außer natürlich für $n = 2, 6$). Die ursprüngliche Methode ([10], [11]) ist lang und unterscheidet eine Vielzahl von Fällen. In diesem Abschnitt skizzieren wir daher einen eleganteren Beweis von Zhu Lie [37]. Er basiert auf der Prolongation und etwas Zahlentheorie.

Wir beginnen mit zwei lateinischen Quadraten der Ordnungen p und q, wobei p eine Primzahl ist und $2q < p$, und konstruieren daraus ein lateinisches Quadrat der Ordnung $p + q$. Sei $L = (a_{ij})$ das lateinische Quadrat mit den Elementen $a_{ij} = i+\lambda j \in \mathbb{Z}_p$, $i, j = 0, 1, \ldots, p-1$, und $\lambda \neq 0, -1$. Bei einem solchen lateinischen Quadrat gibt es eine leicht zu findende Zerlegung in disjunkte Transversalen, und zwar die gebrochenen Diagonalen von links nach rechts. Eine gebrochene Diagonale beginnt in der ersten Spalte und führt diagonal nach rechts unten, bis die letzte Zeile erreicht ist. Dort springt sie in die erste Zeile und führt weiter bis zum unteren Rand. Als Beispiel betrachten wir das folgende lateinische Quadrat, bei dem die eingefärbten Zellen eine gebrochene Diagonale bilden.

$*$	0	1	2	3	4
0	0	2	4	1	3
1	1	3	0	2	4
2	2	4	1	3	0
3	3	0	2	4	1
4	4	1	3	0	2

Die gebrochenen Diagonalen sind eindeutig durch die Startzelle festgelegt. Daher sprechen wir auch von der k-ten gebrochenen Diagonalen, wobei wir damit die Transversale (α_k, Id) mit $\alpha_k(x) =_p k + x$ bezeichnen.

Wir wählen nun q dieser Transversalen aus und bilden damit einen Vektor $K = (k_1, \ldots, k_q)$. Durch beliebige Permutation der Elemente erhalten wir einen zweiten Vektor $K' = (k'_1, \ldots, k'_q)$.

Mit dieser Wahl führen wir die im vorherigen Abschnitt beschriebene Prolongation von Yamamoto durch, wobei wir die gebrochenen Diagonalen gemäß der Vektoren K bzw. K' am unteren bzw. rechten Rand anordnen.

Damit haben wir ein lateinisches Quadrat der Ordnung $p+q$. Sinn muss es aber sein, ein Paar orthogonaler lateinischer Quadrate zu konstruieren. Dazu betrachten wir die beiden lateinischen Quadrate L_a und L_b der Ordnung p, p prim, mit $a \neq b$ und $a, b \neq 0, -1$ mit den Einträgen $(a_{ij}) = i + aj$ bzw. $(b_{ij}) = i + bj$. Weiterhin sei q eine positive ganze Zahl, für die ein Paar orthogonaler lateinischer Quadrate der Ordnung q existiert und $2q < p$. Ebenso sei $K = (k_1, \ldots, k_q)$, $K' = (k'_1, \ldots, k'_q)$ bzw. $M = (m_1, \ldots, m_q)$, $M' = (m'_1, \ldots, m'_q)$ eine Auswahl gebrochener Diagonalen von L_a bzw. L_b. Mit der Prolongation erhalten wir die lateinischen Quadrate L_a^* und L_b^*, beide der Ordnung $p + q$.

Theorem 4.3 *Sei H ein Vektor aus $2q$ verschiedenen Elementen von K und M in beliebiger Reihenfolge. Außerdem sei H^+ der Vektor aus den ersten q und H^- der Vektor aus den letzten q Elementen von H. Falls es ein H gibt mit*

$$(1 + b)K - (1 + a)M = (b - a)H^+ \quad \textit{und}$$

$$(1 + b)(-aK') - (1 + a)(-bM') = (b - a)H^-,$$

dann sind L_a^* und L_b^* orthogonal.

Beweis Die Paare (a^*_{ij}, b^*_{ij}) der durch die Konstruktion neu entstandenen Zeilen sind

$$(k_t + (1 + a)j, m_t + (1 + b)j), \text{ mit } t = 1, \ldots, q \text{ und } j = 0, \ldots, p - 1$$

und die der Spalten

$$(-ak'_t + (1 + a)j, -bm'_t + (1 + b)j), \text{ mit } t = 1, \ldots, q \text{ und } j = 0, \ldots, p - 1.$$

Das sind die einzigen geordneten Paare alter Elemente, die durch die Konstruktion entstehen. Es fallen allerdings auch alte Paare weg. Wenn wir mit h_t die Elemente aus H^+ und mit h'_t die Elemente aus H^- bezeichnen, dann sind die entfallenen Paar gegeben durch

$$(h_t + (1 + a)s, h_t + (1 + b)s) \text{ und } (h'_t + (1 + a)s, h'_t + (1 + b)s)$$

für $t = 1, \ldots, q$ und $s = 0, \ldots, p - 1$. Die beiden lateinischen Quadrate sind dann orthogonal, falls die entfallenen und die neu entstandenen Paare gleich sind. Falls

$$h_t + (1 + a)s = k_t + (1 + a)j \text{ und } h_t + (1 + b)s = m_t + (1 + b)j \text{ sowie}$$

$$h'_t + (1 + a)s = -ak'_t + (1 + a)j \text{ und } h'_t + (1 + b)s = -bm'_t + (1 + b)j$$

gilt, dann ist dies der Fall. Löst man die Gleichungen nach s und dann nach h_t bzw. h'_t auf, so erhält man

$$(b-a)h_t = (1+b)k_t - (1+a)m_t \quad \text{bzw.} \quad (b-a)h'_t = (1+b)(-a)k'_t - (1+a)(-b)m'_t$$

Diese Gleichungen sind nach Voraussetzung für alle t erfüllt. □

Lemma 4.1 *Für jede Primzahl p, $p \geq 7$, $p \equiv 1 \mod 3$, existiert ein Wert μ, so dass $\mu^3 =_p 1$ und $\mu \neq 1, \frac{1}{2}$. Ist p prim, $p > 7$, $p \equiv 2 \mod 3$, dann gibt es ein μ mit $\mu^3 =_p 10$.*

Nach Fermats Theorem gilt $a^{p-1} =_p 1$ für alle a, p prim. Falls $p = 3k+1$, folgt also $a^{3k} =_p 1$ und damit ist $\mu = a^k$ eine Lösung der Gleichung $\mu^3 =_p 1$. Eine zweite Lösung ist $\mu = a^{2k}$. Ist $a \neq 1$, dann sind diese Lösungen die Nullstellen des Polynoms $\mu^2 + \mu + 1 = 0$. Es ist $\mu = 1/2$ aber nur dann eine Nullstelle, wenn $7/4 = 0$ gilt, das kann jedoch nur sein, wenn $p = 7$ ist. Für diese Primzahl ist aber $\mu = 2$ eine Lösung.

Im Fall $p = 3k-1$ sei α ein erzeugendes Element von $\mathbb{Z}_p$ und $b = \alpha^t$ ein beliebiges, von Null verschiedenes Element. Hat b eine 3. Wurzel α^x in $\mathbb{Z}_p$, also $\alpha^{3x} =_p \alpha^t$, dann gilt $3x =_{p-1} t$, denn die multiplikative Gruppe ist zyklisch mit Ordnung $p-1$. Für jedes t gibt es eine eindeutig bestimmte Lösung, denn aus $3x =_p 3y$ folgt $x = y$, da 3 $p-1$ nicht teilt. Damit sind die Elemente $1^3, 2^3, \ldots, (p-1)^3$ alle verschieden. Falls $p \geq 11$, muss es also auch ein Element μ mit $\mu^3 = 10$ geben. □

Theorem 4.4 *Sei $p \equiv 1 \mod 3$ oder $p \equiv 2 \mod 3$ prim, $p \geq 7$, dann existiert ein Paar orthogonaler lateinischer Quadrate der Ordnung $p+3$.*

Beweis Im ersten Fall $p \equiv 1 \mod 3$ gibt es ein μ mit $\mu^3 = 1$ und $\mu \neq 1, \frac{1}{2}$. Sei $a = \frac{\mu-1}{\mu}$ und $b = \frac{\mu}{\mu-1} = \frac{1}{a}$. Weiterhin sei $K = K' = (1, \mu, \mu^2)$ und $M = -\mu K, M' = -\frac{1}{\mu}K$. Mit $H^+ = \mu^2 K$ und $H^- = M$ sind die Bedingungen von Theorem 4.3 erfüllt.

Im zweiten Fall $p \equiv 1 \mod 3$ existiert ein μ mit $\mu^3 = 10$. Wir wählen $a = -3, b = -\frac{1}{3}(1+2\mu), K = K' = (0, 1, \alpha), M = (c, d, e)$ und $M' = (c, e, d)$, wobei $d = -\frac{1}{2}(1+b), c = (1+b)(3+b)/4b, \alpha = (1+b)/2b$ und $e = 1 + (b^2-1)/4b$. Dann sind mit $H^+ = (\alpha, 0, 1)$ und $H^- = (d, c, e)$ die Bedingungen von Theorem 4.3 erfüllt. □

Theorem 4.5 *Für jede Zahl $v = 4t+2 > 6$ existiert ein Paar orthogonaler lateinischer Quadrate der Ordnung v.*

Beweis Wir unterscheiden zwei Fälle. Zunächst sei v kein Vielfaches von 3. In diesem Fall ist $v - 3 = 4t - 1$ nicht durch 3, aber durch eine Primzahl p der Form

$4s-1$ teilbar (denn das Produkt $(4r+1)(4s+1)$ hat die Form $4t+1$) und es gilt somit $p \geq 7$. Also hat v die Darstellung $v = pm+3$. Ist $m = 1$, so haben wir ein Paar orthogonaler lateinischer Quadrate der Ordnung v mit Theorem 4.4. Für $m > 1$ und weil m ungerade ist, erhalten wir ein Paar der Ordnung v durch das singulär direkte Produkt.

Falls v durch 3 teilbar ist, können wir $v = u \cdot 3^h$ schreiben, wobei u nicht durch 3 teilbar ist. Ist $u = 2(2k+1) > 2$, so gibt es gemäß vorigem Fall ein Paar orthogonaler lateinischer Quadrate der Ordnung u und damit auch der Ordung v (Konstruktion mit dem direkten Produkt). Ist $u = 2$, also $v = 2 \cdot 3^h > 6$, dann ist $v = 18 \cdot 3^{h-2}$. Wir erhalten ein Paar orthogonaler lateinischer Quadrate der Ordnung 18, indem wir $p = 13, q = 5$ und $K = (1,2,3,4,5), K' = (4,1,2,3,5), M = -K', M' = -K$ mit $H^+ = (3,-2,5,-1,-4)$ und $H^- = (-3,2,-5,1,4)$ wählen. Mit dem direkten Produkt erhalten wir dann ein Paar orthogonaler lateinischer Quadrate der Ordnung v. □

Kapitel 5

Total anti-symmetrische Quasigruppen

Eine Quasigruppe $(Q, *)$ heißt total anti-symmetrisch oder TA-Quasigruppe, wenn

1. $(c * x) * y = (c * y) * x \;\Rightarrow\; x = y$
2. $x * y = y * x \;\Rightarrow\; x = y$

für alle $c, x, y \in Q$ gilt. Ist nur die erste Bedingung erfüllt, so nennen wir sie schwach total anti-symmetrisch oder kurz WTA-Quasigruppe.

Während es leicht ist, total anti-symmetrische Quasigruppen der Ordnung n für $n \neq 4k+2$ zu finden, kann man die Frage, ob TA-Quasigruppen der Ordnung 10 oder im Allgemeinen der Ordnung $4k+2$ existieren, nicht so einfach beantworten. 1986 suchten Ecker und Poch [24] nach TA-Quasigruppen der Ordnung 10. Sie berechneten die Anzahl der total anti-symmetrischen Links-Loops bis Ordnung 6 und untersuchten, wie viele dieser Loops die Sprung-Transpositionen erkennen können:

Ord.	Anzahl Links-Loops	total anti-symmetrisch	erkennt Sprung-Transpositionen
2	1	0	0
3	2	1	0
4	24	2	2
5	1.344	18	12
6	1.128.960	0	0

Sie konnten nicht weiter als bis $n = 6$ rechnen, weil die Anzahl der Quasigruppen stark mit der Ordnung zunimmt. Aufgrund der Tatsache, dass sie keine TA-Quasigruppen der Ordnung 2 und 6 fanden, vermuteten Ecker und Poch, dass

es keine TA-Quasigruppen der Ordnung $4k + 2$ gibt. Dass auf Grundlage dieser beiden Fälle eine solche Vermutung sehr gewagt ist, zeigt die bekannte Eulersche Vermutung zur Existenz paarweise orthogonaler lateinischer Quadrate. Es dauerte zwar fast zwei Jahrhunderte, aber sie wurde schließlich vollständig widerlegt. Die Vermutung von Ecker und Poch erwies sich ebenso als falsch, wie wir im folgenden zeigen werden. Dazu erarbeiten wir zunächst verschiedene Konstruktionen für TA-Quasigruppen.

5.1 Einfache Konstruktionen

5.1.1 Ringe

Sei $(R, +, \cdot)$ ein endlicher kommutativer Ring mit Eins. Falls a und b Einheiten sind, definiert $x * y := ax + by$ eine Quasigruppe. Diese Quasigruppe ist genau dann total anti-symmetrisch, wenn $a - 1$ und $a - b$ Einheiten sind. Um dies zu sehen, nehmen wir an, es gelte

$$(c * x) * y = a(ac + bx) + by = a(ac + by) + bx = (c * y) * x.$$

Durch Umformung erhalten wir $abx + by = aby + bx$, was äquivalent zu $(a-1)x = (a-1)y$ bzw. $x = y$ ist. Gilt $x * y = ax + by = ay + bx = y * x$, so haben wir $(a - b)x = (a - b)y$ und somit $x = y$.

Wählen wir $b = 1$, so reicht die Forderung, dass a und $a - 1$ Einheiten sind, damit $x * y := ax + y$ eine TA-Quasigruppe ist.

Beispiel 5.1 *Im Ring $(\mathbb{Z}_n, +, \cdot)$, n ungerade, wählen wir $a := -1$ und $b := 1$, dann ist $(\mathbb{Z}_n, *)$ mit $x * y := -x + y$ eine TA-Quasigruppe der Ordnung n.*

Beispiel 5.2 *Im Galois Körper $\mathrm{GF}(p^n)$ mit $p^n > 2$ Elementen gibt es ein Element $a \neq 0, 1$. Damit sind a und $a - 1$ Einheiten und $x * y := ax + y$ definiert eine TA-Quasigruppe der Ordnung p^n.*

5.1.2 Isotopie

Betrachten wir die Konstruktion mit einem Ring genauer, so sehen wir, dass wir im Wesentlichen die additive Gruppe des Rings benutzen. Die Multiplikation dient nur dazu, eine Permutation der Elemente zu definieren. Eine Verallgemeinerung ist daher die Betrachtung der zu einer Gruppe $(G, \cdot)$ isotopen Quasigruppen $(Q, *)$ mit $x * y := \gamma(\alpha(x) \cdot \beta(y))$. Das folgende Ergebnis stellt den Zusammenhang von TA-Quasigruppen mit den anti-symmetrischen Abbildungen her.

Lemma 5.1 *Sei $(G, \cdot)$ eine Gruppe, α, β, γ Permutationen und $\alpha \circ \beta^{-1}$ sowie $x \mapsto \alpha \circ \gamma(c \cdot x)$ anti-symmetrische Abbildungen von G für alle $c \in G$, dann ist $(G, *)$ mit $x * y := \gamma(\alpha(x) \cdot \beta(y))$ eine total anti-symmetrische Quasigruppe.*

Beweis Wir nehmen an, es gelte $(c * x) * y = (c * y) * x$, also

$$\gamma(\alpha(\gamma(\alpha(c) \cdot \beta(x))) \cdot \beta(y)) = \gamma(\alpha(\gamma(\alpha(c) \cdot \beta(y))) \cdot \beta(x)).$$

Dies ist äquivalent zu $\alpha \circ \gamma(\alpha(c) \cdot \beta(x)) \cdot \beta(y) = \alpha \circ \gamma(\alpha(c) \cdot \beta(y)) \cdot \beta(x)$. Nach Voraussetzung folgt $\beta(x) = \beta(y)$ bzw. $x = y$.

Ist $x * y = \gamma(\alpha(x) \cdot \beta(y)) = \gamma(\alpha(y) \cdot \beta(x)) = y * x$, so folgt $\alpha \circ \beta^{-1}(\beta(x)) \cdot \beta(y) = \alpha \circ \beta^{-1}(\beta(y)) \cdot \beta(x)$ und nach Voraussetzung $\beta(x) = \beta(y)$ bzw. $x = y$. □

Ganz analog zeigt man das folgende Lemma.

Lemma 5.2 *Sei $(Q, \cdot)$ eine WTA-Quasigruppe, α, β Permutationen von Q, dann ist $(Q, *)$ mit $x * y := \alpha^{-1}(\alpha(x) \cdot \beta(y))$ eine WTA-Quasigruppe.*

Mit $\alpha = \mathrm{Id}$ sehen wir, dass durch das Vertauschen der Spalten einer WTA-Quasigruppe immer wieder eine WTA-Quasigruppe entsteht.

Die Zeilen hingegen können nicht beliebig vertauscht werden. Dazu betrachten wir die WTA-Quasigruppe $x * y :=_n -x + y$, n ungerade. Wir vertauschen die Zeilen, indem wir die Permutation $\alpha : x \mapsto -x$ auf die erste Stelle anwenden, also $x *' y := \alpha(x) * y = -(-x) + y = x + y$. Offensichtlich ist $x *' y = x + y$ keine WTA-Quasigruppe.

Existiert eine WTA-Quasigruppe der Ordnung n, so erhalten wir durch das Umsortieren der Spalten eine WTA-Quasigruppe mit Links-Eins. Eine WTA-Quasigruppe mit Links-Eins erfüllt aber auch die Bedingung $x * y = y * x \Rightarrow x = y$, d.h. sie ist eine TA-Quasigruppe der Ordnung n. Damit gilt:

Theorem 5.1 *Es existiert eine TA-Quasigruppe der Ordnung n genau dann, wenn eine WTA-Quasigruppe der Ordnung n existiert.*

5.1.3 Konjugation

Lemma 5.3 *Sei $(Q, *)$ eine WTA-Quasigruppe, so ist auch $(Q, /)$ eine WTA-Quasigruppe.*

Beweis Es gelte $(c/x)/y = (c/y)/x$. Wir multiplizieren mit y und x von rechts und erhalten $c = (((c/y)/x) * y) * x$. Nun sei $c' := (c/y)/x$ bzw. $c = (c' * x) * y$, dann gilt $(c' * x) * y = (c' * y) * x)$ und es folgt $x = y$, weil $(Q, *)$ eine WTA-Quasigruppe ist. □

5.1.4 Distributive Quasigruppen

Lemma 5.4 *Eine distributive Quasigruppe ist eine WTA-Quasigruppe.*

Beweis Sei $(Q, *)$ eine distributive Quasigruppe. Wir nehmen an, es gilt $(c * x) * y = (c * y) * x$, wodurch $(c * x) * y = (c * y) * (x * y) = (c * y) * x$ folgt. Damit erhalten wir $x * y = x$ und da distributive Quasigruppen idempotent sind $x = y$. □

Bemerkung Distributive Quasigruppen gibt es nur für Ordnungen $n \neq 4k + 2$.

5.1.5 Direktes Produkt

Da sich die Implikationen $x*y = y*x \Rightarrow x = y$ und $(c*x)*y = (c*y)*x \Rightarrow x = y$ auf das direkte Produkt übertragen, gilt:

Lemma 5.5 *Das direkte Produkt zweier TA-Quasigruppen ist wieder eine TA-Quasigruppe.*

Mit dem direkten Produkt haben wir eine einfache Konstruktion von TA-Quasigruppen für ungerade oder durch 4 teilbare Ordnungen:

Lemma 5.6 *Total anti-symmetrische Quasigruppen der Ordnung n existieren für* $n \equiv 0, 1, 3 \mod 4$.

Beweis Ist n ungerade, dann definieren wir $x*y := -x+y$ in $\mathbb{Z}_n$. Ist $n = 2^k$, $k > 1$, dann sei $x * y := ax + y$, $a \neq 0, 1$, wobei wir im Galois-Körper $\mathrm{GF}(2^k)$ rechnen. Das direkte Produkt zweier TA-Quasigruppen ist wieder total anti-symmetrisch. Daher definieren wir für den verbleibenden Fall $n = 2^k u$, $k > 1$, u ungerade, eine Quasigruppe auf $\mathrm{GF}(2^k) \times \mathbb{Z}_u$ durch $(x_1, x_2) * (y_1, y_2) := (ax_1 + y_1, -x_2 + y_2)$. In allen Fällen ist $(Q, *)$ eine TA-Quasigruppe. □

Offen bleiben dagegen die geraden, aber nicht durch 4 teilbaren Ordnungen $n = 4k + 2$. Im nächsten Abschnitt zeigen wir, dass die nahe liegende Ansätze hier nicht zum Erfolg führen können.

5.2 Existenz einer Transversalen

Eine große Anzahl Quasigruppen kann nicht total anti-symmetrisch sein, weil sie eine wichtige Eigenschaft von TA-Quasigruppen nicht erfüllen. Diese Eigenschaft beweisen wir im folgenden Lemma.

Lemma 5.7 *Eine endliche total anti-symmetrische Quasigruppe besitzt eine Transversale.*

Beweis Sei $(Q, *)$ eine TA-Quasigruppe. Wir definieren $\alpha(i) := i$ und $\beta(i) := i\backslash i$ und zeigen, dass (α, β) eine Transversale ist. Es ist klar, dass $\alpha = \mathrm{Id}$ und $\alpha * \beta = \mathrm{Id}$ Permutationen sind. Wenn $\beta(i) = i\backslash i = j\backslash j$ ist, dann sei $x := \beta(i)$ und $y := i\backslash j$ (also $i * x = i$, $j * x = j$ und $i * y = j$). Damit haben wir

$$(i * x) * y = i * y = j = j * x = (i * y) * x.$$

Es folgt $x = y$ bzw. $\beta(i) = i\backslash i = i\backslash j$ und damit $i = j$. Also ist β injektiv und ebenfalls eine Permutation. Somit ist (α, β) eine Transversale. □

Nun können wir die Quasigruppen, die keine Transversale besitzen, ausschließen.

Theorem 5.2 *Die folgenden Quasigruppen sind nicht total anti-symmetrisch.*

1. *Quasigruppen der Ordnung $4k + 2$ mit einem lateinischen Unterquadrat der Ordnung $2k + 1$*
2. *Quasigruppen, die isotop zu einer Gruppe der Ordnung $4k + 2$ sind.*
3. *Quasigruppen der Ordnung $n = mp$ vom p-Stufen Typ, falls m gerade und p ungerade ist.*

Wir zeigen zunächst:

Lemma 5.8 *Sei $(Q, *)$ eine endliche Quasigruppe mit einem Homomorphismus $\varphi : Q \to G$ auf eine abelsche Gruppe $(G, \cdot)$ mit genau einem Element der Ordnung 2 (also mit zyklischer 2-Sylowgruppe) und*

$$\mathit{Kern}\ \varphi := \{x \in Q | \varphi(x) = e\},$$

wobei e das neutrale Element der Gruppe ist, bestehe aus einer ungeraden Anzahl von Elementen. Dann haben alle zu $(Q, *)$ konjugierten oder isotopen Quasigruppen (und insbesondere $(Q, *)$ selbst) keine Transversale und sind nicht total anti-symmetrisch.

Beweis Seien $(Q, *)$ eine Quasigruppe mit einem Homomorphismus φ auf die abelsche Gruppe $(G, \cdot)$, a das einzige Element der Ordnung 2 in G und $p = |\mathrm{Kern}\ \varphi|$ ungerade. Weil $\varphi((x * y) * z) = \varphi(x * (y * z))$ und $\varphi(x * y) = \varphi(y * x)$, schreiben

wir $\varphi(\prod_{x\in Q} x)$ und kümmern uns nicht um die Klammern oder die Reihenfolge der Elemente im Produkt.

Wir nehmen an, dass Q total anti-symmetrisch ist, also besitzt Q eine Transversale (α, β) mit den Permutationen α, β und $\alpha * \beta$. Außer für e und a gibt es genau ein inverses Element $g^{-1} \neq g$ für jedes Element $g \in G$. Damit folgt

$$\begin{aligned}\varphi(\prod_{x\in Q} x) &= \prod_{x\in Q} \varphi(x) = \prod_{g\in G} g^p \\ &= e^p \cdot a^p \cdot (g_1 \cdot g_1^{-1})^p \cdot \ldots \cdot (g_k \cdot g_k^{-1})^p = a^p = a\end{aligned}$$

und

$$\begin{aligned}\varphi(\prod_{x\in Q} x) &= \varphi(\prod_{x\in Q} \alpha(x) * \beta(x)) = \prod_{x\in Q} \varphi(\alpha(x)) \prod_{x\in Q} \varphi(\beta(x)) \\ &= \prod_{x\in Q} \varphi(x) \prod_{x\in Q} \varphi(x) = \varphi(\prod_{x\in Q} x) \cdot \varphi(\prod_{x\in Q} x) \\ &= a \cdot a = e,\end{aligned}$$

also ein Widerspruch. Das zeigt, dass Q keine Transversale besitzt und damit auch nicht total anti-symmetrisch sein kein. Wie man leicht sieht, überträgt sich die Eigenschaft, eine Transversale zu besitzen, auf alle isotopen und konjugierten Quasigruppen. □

Beweis des Theorems zu 1) Wenn wir eine Quasigruppe der Ordnung $4k+2$ mit einem lateinischen Unterquadrat der Ordnung $2k+1$ haben, können wir die Zeilen und Spalten umordnen, so dass wir eine Unterquasigruppe U von Q erhalten. Nun definieren wir einen Homomorphismus $\varphi : (Q, *) \to (\mathbb{Z}_2, +)$ durch

$$\varphi(x) := \begin{cases} 0 & \text{falls } x \in U \\ 1 & \text{sonst.} \end{cases}$$

Dann ist $|\text{Kern } \varphi| = 2k+1$ und die Behauptung folgt durch das Lemma.

zu 2) Jede Gruppe der Ordnung $4k+2$ hat eine Untergruppe der Ordnung $2k+1$ (siehe z.B. [18]), so dass jede Quasigruppe, die isotop zu einer Gruppe der Ordnung $4k+2$ ist, ein lateinisches Unterquadrat der Ordnung $2k+1$ hat. Mit 1) folgt die Behauptung.

zu 3) Dieser Punkt entspricht Theorem 12.3.1. in Denes/Keedwell [21]: eine Quasigruppe der Ordnung $n = mp$ vom p-Stufen Typ hat keine Transversale, falls

m gerade und p ungerade ist. Eine solche Quasigruppe besitzt einen Homomorphismus auf $\mathbb{Z}_m$, und die Anzahl der Elemente im Kern ist p. □

Das Theorem zeigt, dass wir durch die nahe liegenden Ansätze keine TA-Quasigruppe der Ordnung $4k + 2$ finden können.

5.3 Prolongation

Wir untersuchen nun, unter welchen Bedingungen wir mit Hilfe der Prolongation TA-Quasigruppen konstruieren können. Dazu sei eine WTA-Quasigruppe $(Q, *)$, $Q = \{0, 1, \ldots, n-1\}$, der Ordnung n mit einer Transversalen T gegeben. Falls die per Prolongation konstruierte Quasigruppe ebenfalls eine WTA-Quasigruppe ist, so gilt dies auch, wenn wir die Spalten vor oder nach der Konstruktion beliebig vertauschen. Wir ordnen daher die Spalten um, so dass die Transversale auf der Diagonalen liegt. Dadurch vereinfacht sich die Definition der Quasigruppe $(Q', \cdot)$, $Q' := Q \cup \{n\}$ wie folgt:

$$x \cdot y := \begin{cases} x * y & x, y < n \text{ und } x \neq y \\ x * x & x < n, y = n \\ y * y & x = n, y < n \\ n & x = y. \end{cases}$$

Wie wir sehen, gilt für diese Quasigruppe $n \cdot x = x \cdot n$, daher ist sie nicht total anti-symmetrisch, wir können die Konstruktion aber mit WTA-Quasigruppen durchführen.

Lemma 5.9 *Genau dann erhält man aus einer WTA-Quasigruppe $(Q, *)$ mit der Insertion-Konstruktion eine WTA-Quasigruppe $(Q', \cdot)$, wenn für $x \neq y$, $x, y \in Q$, gilt:*

a) $x \neq x * x$ *und* $x \neq (x * x) * (x * x)$

b) $x * y = x$ *oder* $x * y = y$ *oder* $x * (x * y) \neq y$

c) $x * y = x$ *oder* $y * y \neq (x * y) * x$

d) $y = x * x$ *oder* $x = y * y$ *oder* $(x * x) * y \neq (y * y) * x$

e) $y = x * x$ *oder* $(x * x) * y \neq (x * y) * (x * y)$

Beweis 1. Seien $(Q, *)$ und $(Q', \cdot)$ WTA-Quasigruppen. Zu zeigen: Bedingungen *a)-e)* gelten. (Bed. *a)-e)* sind notwendig.)

Annahme Bed. *a)* gilt nicht: Es existiert ein $x \in Q$ mit $x = x * x$ oder $x = (x * x) * (x * x)$. Falls $x = x * x$, setzen wir $c := y := n$. Es folgt

$$\begin{aligned}(c \cdot x) \cdot y &= (n \cdot x) \cdot n \\ &= (x * x) \cdot n \\ &= (x * x) * (x * x) \\ &= x * x \\ &= n \cdot x \\ &= (n \cdot n) \cdot x \\ &= (c \cdot y) \cdot x\end{aligned}$$

Widerspruch.

Falls $x \neq x*x$ und $x = (x*x)*(x*x)$, setzen wir $y := x*x$ und $c := n$, dann ist

$$\begin{aligned}(c \cdot x) \cdot y &= (n \cdot x) \cdot (x * x) \\ &= (x * x) \cdot (x * x) \\ &= n \\ &= x \cdot x \\ &= ((x * x) * (x * x)) \cdot x \\ &= (y * y) \cdot x \\ &= (n \cdot y) \cdot x \\ &= (c \cdot y) \cdot x\end{aligned}$$

Widerspruch.

Annahme Bed. *b)* gilt nicht: Es gibt $c \neq y$ mit $c * y \neq c$, $c * y \neq y$ und $c * (c * y) = y$. Wir setzen $x := c * y$, dann ist

$$\begin{aligned}(c \cdot x) \cdot y &= (c \cdot (c * y)) \cdot y \\ &= (c * (c * y)) \cdot y \\ &= y \cdot y \\ &= n \\ &= x \cdot x \\ &= (c * y) \cdot x \\ &= (c \cdot y) \cdot x\end{aligned}$$

Widerspruch.

Annahme Bed. *c)* gilt nicht: Für $x \neq y$ gelte $x * y \neq x$ und $y * y = (x * y) * x$. Sei $c := x$, es folgt

$$\begin{aligned}(c \cdot x) \cdot y &= (x \cdot x) \cdot y \\ &= n \cdot y \\ &= y * y \\ &= (x * y) * x \\ &= (c \cdot y) \cdot x\end{aligned}$$

Widerspruch.

Annahme Bed. *d)* gilt nicht: $y \neq x*x$ und $x \neq y*y$ und $(x*x)*y = (y*y)*x$. Sei $c := n$, dann ist

$$\begin{aligned}(c \cdot x) \cdot y &= (n \cdot x) \cdot y \\ &= (x * x) \cdot y \\ &= (x * x) * y \\ &= (y * y) * x \\ &= (c \cdot y) \cdot x\end{aligned}$$

Widerspruch.

Annahme Bed. *e)* gilt nicht: Für $c \neq y$ gelte $y \neq c * c$ und $(c * c) * y = (c * y) * (c * y)$. Sei $x := n$, dann ist

$$\begin{aligned}(c \cdot x) \cdot y &= (c \cdot n) \cdot y \\ &= (c * c) \cdot y \\ &= (c * c) * y \\ &= (c * y) * (c * y) \\ &= (c * y) \cdot n \\ &= (c \cdot y) \cdot x\end{aligned}$$

Widerspruch.

2. Sei $(Q, *)$ eine WTA-Quasigruppe mit den Eigenschaften *a)-e)*. Zu zeigen: $(Q', \cdot)$ ist eine WTA-Quasigruppe. (Bed. *a)-e)* sind hinreichend.) Wir nehmen $(c \cdot x) \cdot y = (c \cdot y) \cdot x$ an.

- Fall $c, x, y < n$, $c \neq x, y$:

- Falls $c*x = y$, $c*y = x$ so gilt $c*(c*y) = y$. Nach *b)* folgt nun $c*y = c$ oder $c*y = y$ und damit $c = x$ (Widerspruch zur Voraussetzung) oder $x = y$.
- Falls $c*x \neq y$, $c*y = x$ (oder $c*x = y$, $c*y \neq x$) folgt

$$\begin{array}{rrcll} & (c\cdot x)\cdot y & = & (c*x)\cdot y & \\ & & = & (c*x)*y & = \\ & (c\cdot y)\cdot x & = & (c*y)\cdot x & \\ & & = & n & \\ \Leftrightarrow & (c*x)*y & = & n & \end{array}$$

  Widerspruch, denn $(c*x)*y \in Q$, aber $n \notin Q$.
- Falls $c*x \neq y$, $c*y \neq x$, dann folgt, da $(Q,*)$ eine WTA-Quasigruppe ist,

$$\begin{array}{rrcll} & (c\cdot x)\cdot y & = & (c*x)*y & = \\ & (c\cdot y)\cdot x & = & (c*y)*x & \\ \Leftrightarrow & x & = & y. & \end{array}$$

- Fall $c, x, y < n$, $c = x$, $c \neq y$ (oder $c \neq x$, $c = y$):
  - Falls $c*y = x$, gilt

$$\begin{array}{rrcll} & (c\cdot x)\cdot y & = & n\cdot y & \\ & & = & y*y & = \\ & (c\cdot y)\cdot x & = & (c*y)\cdot x & \\ & & = & n & \\ \Leftrightarrow & y*y & = & n. & \end{array}$$

    Widerspruch, denn $y*y \in Q$ aber $n \notin Q$.
  - Falls $c*y \neq x$, gilt

$$\begin{array}{rrcll} & (c\cdot x)\cdot y & = & n\cdot y & \\ & & = & y*y & = \\ & (c\cdot y)\cdot x & = & (c*y)\cdot x & \\ & & = & (c*y)*x & \\ \Leftrightarrow & y*y & = & (x*y)*x. & \end{array}$$

    Widerspruch zu *c)*.
- Fall $c = n$, $x, y < n$:

- Falls $y = x * x$ und $x = y * y$, folgt $x = (x * x) * (x * x)$ im Widerspruch zu *a)*
- Falls $y \neq x * x$ und $x = y * y$ (oder $y = x * x$, $x \neq y * y$), folgt

$$\begin{array}{rlll} & (c \cdot x) \cdot y & = & (x * x) \cdot y \\ & & = & (x * x) * y \quad = \\ & (c \cdot y) \cdot x & = & (y * y) \cdot x \\ & & = & n \\ \Leftrightarrow & (x * x) * y & = & n. \end{array}$$

  Widerspruch, denn $(x * x) * y \in Q$, aber $n \notin Q$.

- Falls $y \neq x * x$ und $x \neq y * y$, folgt

$$\begin{array}{rlll} & (c \cdot x) \cdot y & = & (x * x) \cdot y \\ & & = & (x * x) * y \quad = \\ & (c \cdot y) \cdot x & = & (y * y) \cdot x \\ & & = & (y * y) * x \\ \overset{d)}{\Leftrightarrow} & x & = & y. \end{array}$$

- Fall $c < n$, $x = n$, $y < n$ (oder $x < n$, $y = n$):
  - Fall $c = y$. Nach *a)* ist $c * c \neq c$ und damit

$$\begin{array}{rlll} & (c \cdot x) \cdot y & = & (c * c) \cdot y \\ & & = & (c * c) * y \quad = \\ & (c \cdot y) \cdot x & = & n \cdot n \\ & & = & n \\ \Leftrightarrow & (c * c) * y & = & n. \end{array}$$

    Widerspruch, denn $(c * c) * y \in Q$, aber $n \notin Q$.

  - Fall $c \neq y$, $y = c * c$.

$$\begin{array}{rlll} & (c \cdot x) \cdot y & = & (c * c) \cdot y \\ & & = & n \quad = \\ & (c \cdot y) \cdot x & = & (c * y) \cdot n \\ & & = & (c * y) * (c * y) \\ \Leftrightarrow & (c * y) * (c * y) & = & n. \end{array}$$

    Widerspruch, denn $(c * y) * (c * y) \in Q$, aber $n \notin Q$.

– Fall $c \neq y$, $y \neq c * c$.

$$\begin{array}{rrcll} & (c \cdot x) \cdot y & = & (c * c) \cdot y & \\ & & = & (c * c) * y & = \\ & (c \cdot y) \cdot x & = & (c * y) \cdot n & \\ & & = & (c * y) * (c * y) & \\ \Leftrightarrow & (c * c) * y & = & (c * y) * (c * y). & \end{array}$$

Widerspruch zu *e)*.

- Fall $c = n$, $x = n$, $y < n$ (oder $x < n$, $y = n$):

  – Es folgt

$$\begin{array}{rrcll} & (c \cdot x) \cdot y & = & n \cdot y & \\ & & = & y * y & = \\ & (c \cdot y) \cdot x & = & (y * y) \cdot n & \\ & & = & (y * y) * (y * y) & \\ \Leftrightarrow & y * y & = & (y * y) * (y * y). & \end{array}$$

Widerspruch zu *a)*.

Damit haben wir $(c \cdot x) \cdot y = (c \cdot y) \cdot x \Rightarrow x = y$ für alle $c, x, y \in Q'$ bewiesen. □

5.3.1 Anwendung der Prolongation bei Ringen

Als Ausgangspunkt für die Anwendung der Prolongation nehmen wir einen kommutativen Ring $(R, +, -, 0, \cdot, 1)$, $R = \{0, 1, \ldots, n-1\}$ mit Eins und definieren die Quasigruppe $(R, *)$ durch $x * y := ax + by + d$, wobei a, b Einheiten in R sind.

Lemma 5.10 *Sei $x * y := ax + by + d$ definiert auf R. Es gelte*

a) $a, a-1, a+b, a+b+1, a^2+ab-b, b, b+1$ und d sind Einheiten in R

b) $1-a-b$ ist Nullteiler oder gleich 0 in R

c) es gibt ein $0_t \in R$, $0_t \neq 0$ mit $0_t(a - ab + b) = 0$ und $0_t(a^2 + b) = 0$,

dann erhält man mit der Insertion-Konstruktion eine WTA-Quasigruppe der Ordnung $n+1$.

Beweis Wir zeigen die Behauptung mit Lemma 5.9. $(R, *)$ mit $x * y := ax + by + d$ definiert eine Quasigruppe genau dann, wenn a, b Einheiten sind. $(R, *)$ ist WTA,

denn es gilt

$$\begin{aligned} & (c*x)*y &=& \ a(ac+bx+d)+by+d \\ & &=& \ a^2c+abx+ad+by+d \\ & &=& \ a^2c+aby+ad+bx+d = (c*y)*x \\ \Leftrightarrow & abx+by &=& \ aby+bx \\ \Leftrightarrow & abx-bx &=& \ aby-by \\ \Leftrightarrow & (a-1)bx &=& \ (a-1)by. \end{aligned}$$

Nach Voraussetzung sind $a-1$ und b Einheiten, also folgt $x=y$.
Die Diagonale ist eine Transversale, denn

$$\begin{aligned} & x*x &=& \ y*y \\ \Leftrightarrow & ax+bx+d &=& \ ay+by+d \\ \Leftrightarrow & (a+b)x &=& \ (a+b)y \\ \Leftrightarrow & x &=& \ y. \end{aligned}$$

Nun prüfen wir die Bedingungen von Lemma 5.9. Dazu seien $x, y \in R$ mit $x \neq y$.

- Bed. *a)*, Teil 1: Zu zeigen $x \neq x*x$. Wir nehmen $x = x*x$ an, es folgt

$$\begin{aligned} & x &=& \ ax+bx+d \\ \Leftrightarrow & (1-a-b)x &=& \ d. \end{aligned}$$

  Ist $1-a-b=0$, dann folgt $d=0$ im Widerspruch zur Voraussetzung, dass d eine Einheit ist. Demnach muss $1-a-b$ ein Nullteiler sein, d.h. es existiert ein $0_{1-a-b} \in R \setminus \{0\}$, mit $0_{1-a-b}(1-a-b)=0$ und damit

$$\begin{aligned} \Rightarrow & 0_{1-a-b}(1-a-b)x &=& \ 0_{1-a-b}d \\ \Leftrightarrow & 0x &=& \ 0_{1-a-b}d \\ \Leftrightarrow & 0 &=& \ 0_{1-a-b} \end{aligned}$$

  Widerspruch.

- Bed. *a)*, Teil 2: Zu zeigen $x \neq (x*x)*(x*x)$. Wir nehmen $x = (x*x)*(x*x)$ an, es folgt

$$\begin{aligned}
& & x &= (ax+bx+d)*(ax+bx+d) \\
& & &= a(ax+bx+d)+b(ax+bx+d)+d \\
& & &= a^2x+abx+ad+abx+b^2x+bd+d \\
\Leftrightarrow & (1-a^2-2ab-b^2)x &= (a+b+1)d \\
\Leftrightarrow & (a+b+1)(1-a-b)x &= (a+b+1)d \\
\Leftrightarrow & (1-a-b)x &= d
\end{aligned}$$

Analog zum ersten Teil folgt ein Widerspruch.

- Bed. *b)*: Wir zeigen $x*(x*y)=y \Rightarrow x*y=y$.

$$\begin{aligned}
& y &= x*(x*y) \\
& &= ax+b(ax+by+d)+d \\
& &= ax+abx+b^2y+bd+d \\
\Leftrightarrow & (1-b^2)y &= (b+1)ax+(b+1)d \\
\Leftrightarrow & (b+1)(1-b)y &= (b+1)ax+(b+1)d \\
\Leftrightarrow & (1-b)y &= ax+d \\
\Leftrightarrow & y &= ax+by+d \\
\Leftrightarrow & y &= x*y
\end{aligned}$$

- Bed. *c)*: Es sei $y*y=(x*y)*x$, d.h.

$$\begin{aligned}
& ay+by+d &= a(ax+by+d)+bx+d \\
\Leftrightarrow & (a+b)y &= a^2x+aby+ad+bx \\
\Leftrightarrow & (a-ab+b)y &= (a^2+b)x+ad \\
\Rightarrow & 0_t(a-ab+b)y &= 0_t(a^2+b)x+0_tad \\
\Leftrightarrow & 0 &= 0+0_tad \\
\Leftrightarrow & 0 &= 0_t
\end{aligned}$$

Widerspruch. Damit haben wir $y*y \neq (x*y)*x$ für alle $x,y \in R$ gezeigt.

- Bed. *d)*: Es sei $(x*x)*y=(y*y)*x$, d.h.

$$\begin{aligned}
& a(ax+bx+d)+by+d &= a(ay+by+d)+bx+d \\
\Leftrightarrow & a^2x+abx+ad+by &= a^2y+aby+ad+bx \\
\Leftrightarrow & (a^2+ab-b)x &= (a^2+ab-b)y \\
\Leftrightarrow & x &= y.
\end{aligned}$$

Also gilt $(x*x)*y \neq (y*y)*x$ für alle $x \neq y$.

- Bed. *e)*: Wir nehmen an, es gelte $(x * x) * y = (x * y) * (x * y)$, also

$$\begin{array}{rrcl} & a(ax+bx+d)+by+d & = & a(ax+by+d)+b(ax+by+d)+d \\ \Leftrightarrow & a^2x+abx+ad+by & = & a^2x+aby+ad+abx+b^2y+bd \\ \Leftrightarrow & (-b^2-ab+b)y & = & bd \\ \Leftrightarrow & (-b-a+1)y & = & d. \end{array}$$

  Analog zu Bedingung *a)* folgt ein Widerspruch.

Damit sind alle Bedingungen von Lemma 5.9 erfüllt und es folgt die Existenz einer WTA-Quasigruppe der Ordnung $n+1$. □

Bei der Suche nach Lösungen für die in Lemma 5.10 für a und b geforderten Voraussetzungen legt es Bedingung *c)* nahe, folgende Ansätze zu untersuchen:

1. Mit $a-ab+b = a^2+b$ wäre Bedingung *c)* bereits erfüllt, wenn $a-ab+b = 0$ oder $a-ab+b$ ein Nullteiler wäre. Aus $a-ab+b = a^2+b$ folgt $ab = a-a^2$ bzw. $b = 1-a$. Damit ist $a-ab+b = a-a+a^2+1-a = a^2-a+1$.

2. Falls $a-ab+b = 0$ ist, ist Bedingung *c)* erfüllt, wenn a^2+b ein Nullteiler ist. Löst man die erste Gleichung nach b auf, erhält man $a = (a-1)b$, also $b = \frac{a}{a-1}$ und $a^2+b = a^2+\frac{a}{a-1} = \frac{a^2(a-1)+a}{a-1} = \frac{a}{a-1}(a^2-a+1)$.

3. Als dritte Möglichkeit bleibt $a^2+b = 0$ bzw. $b = -a^2$. Dann ist $a-a(-a^2)-a^2 = a(a^2-a+1)$.

Für diese 3 Ansätze stellen wir die benötigten Bedingungen in der folgenden Tabelle dar:

	$b = 1-a$	$b = \frac{a}{a-1}$	$b = -a^2$
$a+b$	1	$\frac{a^2}{a-1}$	$a(1-a)$
$a+b+1$	2	$\frac{a^2+a-1}{a-1}$	$a-a^2+1$
a^2+ab-b	$2a-1$	$a(a+1)$	$a^2(2-a)$
$b+1$	$2-a$	$\frac{2a-1}{a-1}$	$(1-a)(a+1)$
$1-a-b$	0	$\frac{a^2-a+1}{1-a}$	$1-a+a^2$

Mit der Wahl $d := 1$ ergibt sich aus Lemma 5.10:

Lemma 5.11 *Es seien $a, a-1$ Einheiten und a^2-a+1 ein Nullteiler oder gleich 0 in R, des Weiteren gelte eine der folgenden Bedingungen:*

1. *$2a-1$, $a-2$ und 2 sind Einheiten in R*
2. *$2a-1$, $a+1$ und a^2+a-1 sind Einheiten in R*
3. *$a-2$, $a+1$ und a^2-a-1 sind Einheiten in R*

dann existiert eine TA-Quasigruppe der Ordnung $n+1$.

Beispiel 5.3 *Sei $n = a^2-a+1$ eine Primzahl und $a \in \mathbb{Z}$, dann existiert eine TA-Quasigruppe der Ordnung $n+1$.*

Ist a^2-a+1 eine Primzahl und $a > 2$, so sind $a, a-1, 2a-1$ und $a-2$ Einheiten in $\mathbb{Z}_n$ und die Voraussetzungen von Lemma 5.11 sind erfüllt.

Die Konstruktion funktioniert aber auch für den speziellen Fall $a = 2$ und $n = 3$, obwohl $a-2$ und $2a-1$ keine Einheiten sind. Die davon betroffenen Bedingungen b) und d) von Lemma 5.9 beweisen wir gesondert. Anhand der folgenden Tabelle sehen wir, dass $x*y = x$ oder $x*y = y$ und $y = x*x$ oder $x = y*y$ für $x \neq y$ gilt.

x	y	$x*y$	$x*x$	$y*y$
0	1	$0 = x$	$1 = y$	2
0	2	$2 = y$	1	$0 = x$
1	2	$1 = x$	$2 = y$	0

Beispiel Mit $a = 2$ erhalten wir mit der Prolongation die Quasigruppe $(Q, \cdot)$:

$*$	0	1	2
0	1	0	2
1	0	2	1
2	2	1	0

$\rightarrow$

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

Wir tauschen die Zeilen 0 und 3 und benennen gleichzeitig 0 und 3 um. Durch Umsortierung der Spalten erhalten wir den TA-Links-Loop $(Q, \cdot'')$ (vgl. Seite 97):

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

$\rightarrow$

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

Beispiel Mit $a = 3$ oder $a = 4$ erhalten wir eine TA-Quasigruppe der Ordnung 8 bzw. 14.

5.3.2 Diagonalmethode

Da wir für die Insertion-Konstruktion eine Quasigruppe mit einer Transversalen benötigen, bieten sich die Quasigruppen an, die mit der Diagonalmethode konstruiert wurden. Bei diesen sind alle gebrochenen Diagonalen Transversalen. Die Anforderungen an die im folgenden benutzte Permutation erscheinen hoch. Sie sind aber gut für eine Computersuche geeignet und erlauben es so, TA-Quasigruppen bis zur Ordnung 28 direkt zu konstruieren.

Lemma 5.12 *Sei $p : \mathbb{Z}_n \to \mathbb{Z}_n$, n ungerade, eine Permutation mit folgenden Eigenschaften:*

a) $p(0) \neq 0$

b) $p(x) - p(y) = x - y$ *impliziert* $x = y$

c) $p(y - p(x)) + p(x) = p(x - p(y)) + p(y)$ *impliziert* $x = y$

d) $x \neq p(0)$ *und* $x \neq -p(0)$ *und* $p(-p(0) + x) - p(-p(0) - x) = x$ *impliziert* $x = 0$

e) $p(x) \neq 0$ *und* $p(-p(x)) + p(x) = x + p(0)$ *impliziert* $x = 0$

f) $p(x) \neq 0$ *und* $p(x) \neq x$ *und* $p(p(x)) = x$ *impliziert* $x = 0$

und $x * y := p(-x + y) + x$ dann erhält man mit der Insertion-Konstruktion eine WTA-Quasigruppe der Ordnung $n + 1$.

Beweis Wir zeigen die Behauptung mit Lemma 5.9. $(\mathbb{Z}_n, *)$ mit $x * y := p(-x + y) + x$ definiert eine Quasigruppe genau dann, wenn $p(x) - p(y) = x - y \Rightarrow x = y$. $(\mathbb{Z}_n, *)$ ist WTA: Wir nehmen an, dass

$$\begin{aligned}(c * x) * y &= p(-p(-c + x) - c + y) + p(-c + x) + c \\ &= p(-p(-c + y) - c + x) + p(-c + y) + c \\ &= (c * y) * x.\end{aligned}$$

Wir setzen $\tilde{x} := -c + x$ und $\tilde{y} := -c + y$, wodurch $p(-p(\tilde{x}) + \tilde{y}) + p(\tilde{x}) = p(-p(\tilde{y}) + \tilde{x}) + p(\tilde{y})$ folgt. Nach Voraussetzung folgt $\tilde{x} = -c + x = -c + y = \tilde{y}$ bzw. $x = y$.
Die Diagonale ist eine Transversale, denn

$$\begin{aligned} & x * x &=& \; y * y \\ \Leftrightarrow \quad & p(-x + x) + x &=& \; p(-y + y) + y \\ \Leftrightarrow \quad & p(0) + x &=& \; p(0) + y \\ \Leftrightarrow \quad & x &=& \; y.\end{aligned}$$

Nun prüfen wir die Bedingungen von Lemma 5.9. Dazu seien $x, y \in \mathbb{Z}_n$ mit $x \neq y$.

- Bed. *a)*, Teil 1: Zu zeigen $x \neq x * x$. Wir nehmen $x = x * x$ an, es folgt

$$\begin{array}{rrcl} & x & = & p(-x+x)+x \\ \Leftrightarrow & x & = & p(0)+x \\ \Leftrightarrow & 0 & = & p(0). \end{array}$$

  Widerspruch.

- Bed. *a)*, Teil 2: Zu zeigen $x \neq (x*x)*(x*x)$. Wir nehmen $x = (x*x)*(x*x)$ an, es folgt

$$\begin{array}{rrcl} & x & = & (p(-x+x)+x)*(p(-x+x)+x) \\ & & = & (p(0)+x)*(p(0)+x) \\ & & = & p(0)+p(0)+x \\ \Leftrightarrow & 0 & = & 2p(0) \\ \Leftrightarrow & 0 & = & p(0). \end{array}$$

  Widerspruch.

- Bed. *b)*: Es sei $x * y \neq x$, $x * y \neq y$ und es gelte $x * (x * y) = y$.

$$\begin{array}{rrcl} & y & = & x*(x*y) \\ & & = & p(-x+p(-x+y)+x)+x \\ & & = & p(p(-x+y))+x \\ \Leftrightarrow & -x+y & = & p(p(-x+y)) \end{array}$$

  Wir setzen $\tilde{x} := -x + y$, dann gilt $p(-x+y)+x \neq x \Leftrightarrow p(\tilde{x}) \neq 0$, $p(-x+y)+x \neq y \Leftrightarrow p(\tilde{x}) \neq \tilde{x}$ und $p(p(\tilde{x})) = \tilde{x}$. Nach Voraussetzung folgt nun $\tilde{x} = -x + y = 0$ und damit $x = y$. Widerspruch.

- Bed. *c)*: Es sei $x*y \neq x$, $y*y = (x*y)*x$ und $\tilde{x} := -x+y$, d.h. $p(\tilde{x}) \neq 0$ und

$$\begin{array}{rrcl} & p(-y+y)+y & = & p(-p(-x+y)-x+x)+p(-x+y)+x \\ \Leftrightarrow & p(0)-x+y & = & p(-p(-x+y))+p(-x+y) \\ \Leftrightarrow & p(0)+\tilde{x} & = & p(-p(\tilde{x}))+p(\tilde{x}). \end{array}$$

  Nach Voraussetzung folgt $\tilde{x} = 0$ bzw. $x = y$. Widerspruch.

- Bed. *d)*: Es sei $y \neq x*x$, $x \neq y*y$ und $(x*x)*y = (y*y)*x$. Mit $\tilde{x} := -x+y$ gilt $\tilde{x} \neq p(0)$, $\tilde{x} \neq -p(0)$ und

$$\begin{aligned} & p(-p(0) - x + y) + p(0) + x &=& \; p(-p(0) - y + x) + p(0) + y \\ \Leftrightarrow\; & p(-p(0) + \tilde{x}) - p(-p(0) - \tilde{x}) &=& \; \tilde{x}. \end{aligned}$$

  Nach Voraussetzung folgt $\tilde{x} = 0$ bzw. $x = y$. Widerspruch.

- Bed. *e)*: Wir nehmen an, es gelte $(x * x) * y = (x * y) * (x * y)$, also

$$\begin{aligned} & p(-p(0) - x + y) + p(0) + x &=& \; (p(-x + y) + x) * (p(-x + y) + x) \\ & &=& \; p(0) + p(-x + y) + x \\ \Leftrightarrow\; & p(-p(0) - x + y) &=& \; p(-x + y) \\ \Leftrightarrow\; & -p(0) - x + y &=& \; -x + y \\ \Leftrightarrow\; & p(0) &=& \; 0. \end{aligned}$$

  Widerspruch.

Damit sind alle Bedingungen von Lemma 5.9 erfüllt und es folgt die Existenz einer WTA-Quasigruppe der Ordnung $n + 1$. □

Beispiel Für Ordnung 18 erhalten wir die folgende TA-Quasigruppe:

*	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
00	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
01	02	03	00	04	07	09	12	01	16	14	17	08	05	11	06	10	15	13
02	03	14	04	00	05	08	10	13	02	17	15	01	09	06	12	07	11	16
03	04	17	15	05	00	06	09	11	14	03	01	16	02	10	07	13	08	12
04	05	13	01	16	06	00	07	10	12	15	04	02	17	03	11	08	14	09
05	06	10	14	02	17	07	00	08	11	13	16	05	03	01	04	12	09	15
06	07	16	11	15	03	01	08	00	09	12	14	17	06	04	02	05	13	10
07	08	11	17	12	16	04	02	09	00	10	13	15	01	07	05	03	06	14
08	09	15	12	01	13	17	05	03	10	00	11	14	16	02	08	06	04	07
09	10	08	16	13	02	14	01	06	04	11	00	12	15	17	03	09	07	05
10	11	06	09	17	14	03	15	02	07	05	12	00	13	16	01	04	10	08
11	12	09	07	10	01	15	04	16	03	08	06	13	00	14	17	02	05	11
12	13	12	10	08	11	02	16	05	17	04	09	07	14	00	15	01	03	06
13	14	07	13	11	09	12	03	17	06	01	05	10	08	15	00	16	02	04
14	15	05	08	14	12	10	13	04	01	07	02	06	11	09	16	00	17	03
15	16	04	06	09	15	13	11	14	05	02	08	03	07	12	10	17	00	01
16	17	02	05	07	10	16	14	12	15	06	03	09	04	08	13	11	01	00
17	01	00	03	06	08	11	17	15	13	16	07	04	10	05	09	14	12	02

5.4 Quasi-direktes Produkt

Das direkte Produkt können wir für Ordnungen $4k+2 = 2u$ nur anwenden, wenn u keine Primzahl, also zerlegbar in u_1u_2 ist und wir bereits eine TA-Quasigruppe der Ordnung $2u_1$ oder $2u_2$ haben. Dies ist aber in der Regel nicht der Fall weshalb wir allgemeinere Konstruktionen benötigen. In diesem Abschnitt betrachten wir eine Konstruktion mit dem quasi-direkten Produkt, die eine Konstruktion für alle durch 6 teilbaren Ordnungen (außer 6 selbst) liefert und den Beweis, dass die Klasse der TA-Quasigruppen keine Varietät ist.

Lemma 5.13 *Seien $(R,+,.)$ ein kommutativer Ring mit Eins, $|R| = u$, und b_1, b_2, $b_3 \in R$ Einheiten. Weiterhin seien $a_1 := \frac{b_3}{b_1}$, $a_2 := \frac{b_3^2 b_2}{b_1^3} = \frac{a_1^2}{a_3}$ und $a_3 := \frac{b_1}{b_2}$. Wenn b_1+b_3, b_1-b_3, a_1-1, a_2-1 und a_2+1 Einheiten sind und $a_1 \neq -1$, dann existiert ein TA-Links-Loop $(Q,\cdot)$ der Ordnung $6u$, für den $(x \cdot 0) \cdot 0 = x \Rightarrow x = 0$ gilt.*

Beweis Es gibt keine TA-Quasigruppe der Ordnung 6. Die Idee bei der folgenden Konstruktion ist, eine Quasigruppe der Ordnung 6 zu nehmen, für die für möglichst viele c, x, y die Bedingung $(c * x) * y = (c * y) * x \Rightarrow x = y$ gilt und dann ein quasi-direktes Produkt zu bilden. Hierzu nehmen wir die TA-Quasigruppe $(\mathbb{Z}_5, -x+2y+1)$ der Ordnung 5 und erhalten durch Prolongation die Quasigruppe $(Q,*)$ der Ordnung 6:

$*$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	2	5	0	4	1	3
2	3	4	1	0	5	2
3	4	3	5	2	0	1
4	5	2	4	1	3	0
5	1	0	3	5	2	4

Für diese gilt $(c * x) * y = (c * y) * x$ nur für folgende $x \neq y$:

c	x	y	$c * x$	$c * y$	$(c * x) * y$	$(c * y) * x$
1	5	2	3	0	5	5
2	1	3	4	0	1	1
3	2	4	5	0	2	2
4	3	5	1	0	3	3
5	4	1	2	0	4	4

und entsprechend, wenn man die Bezeichner x und y vertauscht. Ist also $(c*x)*y = (c*y)*x$, so folgt $x = y$ oder $c*x = 0$ oder $c*y = 0$. Wir definieren nun $(Q \times R, \cdot)$ durch

$$(x,u)\cdot(y,v) := \begin{cases} (x*y, a_1u + b_1v + 1) & \text{falls } x*y \neq 0, x \neq 0 \\ (0, a_2u + b_2v) & \text{falls } x*y = 0 \\ (y, a_3u + b_3v) & \text{falls } x = 0, y \neq 0 \end{cases}$$

und zeigen, dass $(Q \times R, \cdot)$ eine WTA-Quasigruppe mit $(x \cdot 0) \cdot 0 = x \Rightarrow x = 0$ ist. Wir nehmen an, es gelte $((c,t)\cdot(x,u))\cdot(y,v) = ((c,t)\cdot(y,v))\cdot(x,u)$.

Fall 1: $c*x = c*y = 0$ und $c = 0$

Damit gilt $x = y = 0$.

$$\begin{array}{rrcll} & ((0,t)\cdot(0,u))\cdot(0,v) & = & (0, a_2t + b_2u)\cdot(0,v) & \\ & & = & (0, a_2^2t + a_2b_2u + b_2v) & = \\ & ((0,t)\cdot(0,v))\cdot(0,u) & = & (0, a_2^2t + a_2b_2v + b_2u) & \\ \Leftrightarrow & a_2b_2u + b_2v & = & a_2b_2v + b_2u & \\ \Leftrightarrow & (a_2-1)b_2u & = & (a_2-1)b_2v & \\ \Leftrightarrow & u & = & v & \end{array}$$

Also ist $(x,u) = (y,v)$.

Fall 2: $c*x = c*y = 0$ und $c \neq 0$

Damit gilt $x = y \neq 0$.

$$\begin{array}{rrcll} & ((c,t)\cdot(x,u))\cdot(y,v) & = & (0, a_2t + b_2u)\cdot(y,v) & \\ & & = & (y, a_3a_2t + a_3b_2u + b_3v) & = \\ & ((c,t)\cdot(y,v))\cdot(x,u) & = & (x, a_3a_2t + a_3b_2v + b_3u) & \\ \Leftrightarrow & a_3b_2u + b_3v & = & a_3b_2v + b_3u & \\ \Leftrightarrow & (a_3b_2 - b_3)u & = & (a_3b_2 - b_3)v & \\ \Leftrightarrow & (b_1 - b_3)u & = & (b_1 - b_3)v & \\ \Leftrightarrow & u & = & v & \end{array}$$

Also ist $(x,u) = (y,v)$.

Fall 3: $c*x = 0$, $c*y \neq 0$ (oder umgekehrt) und $(c*y)*x = 0$

Es ist $(c*x)*y = 0*y = y = (c*y)*x = 0$ und somit $(c*y)*x = 0 = c*x$ bzw. $c = c*0$. Es folgt $c = 0$ und damit $c*y = 0*0 = 0$ im Widerspruch zu $c*y \neq 0$.

Fall 4: $c*x = 0$, $c*y \neq 0$ (oder umgekehrt) und $(c*y)*x \neq 0$

Es ist $(c*x)*y = 0*y = y = (c*y)*x \neq 0$. Gilt $c = 0$, so folgt $x = 0$ und $x*y = y*x \Rightarrow x = y = 0$ im Widerspruch zu $y \neq 0$. Also ist $c \neq 0$.

$$\begin{aligned}
((c,t)\cdot(x,u))\cdot(y,v) &= (0, a_2t + b_2u)\cdot(y,v)\\
&= (y, a_3a_2t + a_3b_2u + b_3v) \quad =\\
((c,t)\cdot(y,v))\cdot(x,u) &= (c*y, a_1t + b_1v + 1)\cdot(x,u)\\
&= ((c*y)*x, a_1^2t + a_1b_1v + a_1 + b_1u + 1)\\
\Leftrightarrow\quad a_1^2t + a_1b_1v + a_1 + b_1u + 1 &= a_3a_2t + a_3b_2u + b_3v\\
\Leftrightarrow\quad a_1 + 1 &= (a_3a_2 - a_1^2)t + (a_3b_2 - b_1)u + (b_3 - a_1b_1)v
\end{aligned}$$

Widerspruch, denn die rechte Seite der Gleichung ist gleich 0 (nach Voraussetzung), wodurch $a_1 = -1$ folgt.

Fall 5: $c*x, c*y \neq 0$, $(c*x)*y = (c*y)*x = 0$

Es gilt $x = y$. Falls $c = 0$, folgt $(0*x)*x = x*x = 0$ bzw. $x = 0$. Es folgt $c*x = 0*0 = 0$, Widerspruch. Daher gilt $c \neq 0$ und damit

$$\begin{aligned}
((c,t)\cdot(x,u))\cdot(x,v) &= (c*x, a_1t + b_1u + 1)\cdot(x,v)\\
&= (0, a_2a_1t + a_2b_1u + a_2 + b_2v) \quad =\\
((c,t)\cdot(x,v))\cdot(x,u) &= (0, a_2a_1t + a_2b_1v + a_2 + b_2u)\\
\Leftrightarrow\quad a_2b_1u + b_2v &= a_2b_1v + b_2u\\
\Leftrightarrow\quad (a_2b_1 - b_2)u &= (a_2b_1 - b_2)v
\end{aligned}$$

Es ist $a_2b_1 - b_2 = \frac{b_3^2b_2}{b_1^3}b_1 - b_2 = \frac{(b_3^2-b_1^2)b_2}{b_1^2} = \frac{(b_3-b_1)(b_3+b_1)b_2}{b_1^2}$ eine Einheit, daher folgt $u = v$.

Fall 6: $c*x, c*y \neq 0$, $(c*x)*y = (c*y)*x \neq 0$ und $c = 0$

Es gilt $x = y$ und

$$\begin{aligned}
((0,t)\cdot(x,u))\cdot(x,v) &= (x, a_3t + b_3u)\cdot(x,v)\\
&= (x*x, a_1a_3t + a_1b_3u + b_1v + 1) \quad =\\
((0,t)\cdot(x,v))\cdot(x,u) &= (x*x, a_1a_3t + a_1b_3v + b_1u + 1)\\
\Leftrightarrow\quad a_1b_3u + b_1v &= a_1b_3v + b_1u\\
\Leftrightarrow\quad (a_1b_3 - b_1)u &= (a_1b_3 - b_1)v
\end{aligned}$$

$a_1b_3 - b_1 = \frac{b_3}{b_1}b_3 - b_1 = \frac{b_3^2-b_1^2}{b_1} = \frac{(b_3-b_1)(b_3+b_1)}{b_1}$ ist eine Einheit, daher folgt $u = v$.

Fall 7: $c * x, c * y \neq 0$, $(c * x) * y = (c * y) * x \neq 0$ und $c \neq 0$

Es gilt $x = y$ und

$$\begin{aligned} ((c,t)\cdot(x,u))\cdot(x,v) &= (c*x, a_1t + b_1u + 1)\cdot(x,v) \\ &= ((c*x)*x, a_1^2t + a_1b_1u + a_1 + b_1v + 1) \quad = \\ ((c,t)\cdot(x,v))\cdot(x,u) &= ((c*x)*x, a_1^2t + a_1b_1v + a_1 + b_1u + 1) \\ \Leftrightarrow \qquad a_1b_1u + b_1v &= a_1b_1v + b_1u \\ \Leftrightarrow \qquad (a_1-1)b_1u &= (a_1-1)b_1v \end{aligned}$$

$a_1 - 1$ und b_1 sind Einheiten nach Voraussetzung, daher folgt $u = v$.

Damit haben wir bewiesen, dass $(Q \times R, \cdot)$ eine WTA-Quasigruppe ist.

Nun zeigen wir $((x,u)\cdot(0,0))\cdot(0,0) = (x,u) \Rightarrow (x,u) = (0,0)$.

Fall 1: $x = 0$

Es folgt

$$\begin{aligned} ((0,u)\cdot(0,0))\cdot(0,0) &= (0, a_2u)\cdot(0,0) \\ &= (0, a_2^2u) \\ &= (0,u), \end{aligned}$$

also $(a_2^2 - 1)u = (a_2 + 1)(a_2 - 1)u = 0$. Nach Voraussetzung sind $a_2 - 1$ und $a_2 + 1$ Einheiten und es folgt $u = 0$.

Fall 2: $x \neq 0$

Es ist $x * 0 \neq 0$ und $(x * 0) * 0 \neq 0$. Es folgt

$$\begin{aligned} ((x,u)\cdot(0,0))\cdot(0,0) &= (x*0, a_1u + 1)\cdot(0,0) \\ &= ((x*0)*0, a_1^2u + a_1 + 1) \\ &= (x,u), \end{aligned}$$

also gilt $(x * 0) * 0 = x$. Dies kann aber nur gelten, wenn $x = 0$ ist, im Widerspruch zur Annahme $x \neq 0$.

Durch Umordnung der Spalten von $(Q \times R, \cdot)$ erhalten wir den gesuchten TA-Links-Loop. Damit ist das Lemma bewiesen. □

Das quasi-direkte Produkt liefert auch ein weiteres Ergebnis.

Theorem 5.3 *Die Klasse der TA-Quasigruppen definiert keine Varietät.*

Beweis Die Klasse der TA-Quasigruppen ist nicht unter homomorphen Bildern abgeschlossen. Dazu betrachten wir folgendes Beispiel. Sei $n = 6 \cdot 5 = 30$, wir wählen die Einheiten $b_1 = 2$, $b_2 = 1$, $b_3 = 1$ und $a_1 = 3, a_2 = 2, a_3 = 2$ aus $\mathbb{Z}_5$.

Damit sind die Voraussetzungen von Lemma 5.13 erfüllt und es folgt, dass der Links-Loop $(Q \times \mathbb{Z}_5, \cdot)$

$$(x,u)\cdot(y,v) := \begin{cases} (x*y, a_1u + b_1v + 1) & \text{falls } x*y \neq 0, x \neq 0 \\ (0, a_2u + b_2v) & \text{falls } x*y = 0 \\ (y, a_3u + b_3v) & \text{falls } x = 0, y \neq 0 \end{cases}$$

total anti-symmetrisch ist. Offensichtlich definiert aber $\varphi : Q \times \mathbb{Z}_5 \to Q$ mit $\varphi(x,u) := x$ einen Homomorphismus von $(Q \times \mathbb{Z}_5, \cdot)$ nach $(Q, *)$. $(Q, *)$ ist aber eine Quasigruppe der Ordnung 6 und nicht total anti-symmetrisch. □

5.5 Verallgemeinertes singulär direktes Produkt

Es sei $(Q, *)$ eine Quasigruppe mit einer Unterquasigruppe $(S, *)$ und $(V, \bigtriangledown)$ eine idempotente Quasigruppe. Weiterhin sei $P = Q \backslash S$ und $(P, \otimes_{v,w})$ eine Quasigruppe für alle geordneten Paare $(v,w) \in V \times V$ mit verschiedenen Elementen v und w.

Auf der Menge $S \cup (P \times V)$ definieren wir $\cdot$ durch

$$\begin{aligned} x \cdot y &= x * y \\ x \cdot (r,v) &= (x * r, v) \\ (r,v) \cdot y &= (r * y, v) \\ (r,v) \cdot (s,v) &= r * s \text{ falls } r * s \in S \\ (r,v) \cdot (s,v) &= (r * s, v) \text{ falls } r * s \in P \\ (r,v) \cdot (s,w) &= (r \otimes_{v,w} s, v \bigtriangledown w) \text{ falls } v \neq w, \end{aligned}$$

wobei $x, y \in S$, $r, s \in P$ und $v, w \in V$.

Lemma 5.14 *Das verallgemeinerte singulär direkte Produkt definiert eine WTA-Quasigruppe, falls gilt:*

a) $(Q, *)$ *ist WTA.*

b) $(c * x) \otimes_{u,v} y \neq (c \otimes_{u,v} y) * x$, *falls* $u \neq v$, $x \in S$, $(c,u), (y,v) \in P \times V$

c) $v \bigtriangledown w \neq w \bigtriangledown v$ *oder* $(c*x) \otimes_{w,v} y \neq (c*y) \otimes_{v,w} x$ *für* $v \neq w$, $c \in S$, $(x,w), (y,v) \in P \times V$

d) $v \neq (w \bigtriangledown v) \bigtriangledown w$ *oder* $c * x \in P$ *oder* $(c * x) * y \neq (c \otimes_{w,v} y) \otimes_{w \bigtriangledown v, w} x$ *für* $v \neq w$, $(c,w), (x,w), (y,v) \in P \times V$

e) $(c \otimes_{u,w} x) \otimes_{u \triangledown w, w} y = (c \otimes_{u,w} y) \otimes_{u \triangledown w, w} x \Rightarrow x = y$, $u \neq w$, $(c,u),(x,w),(y,w) \in P \times V$

f) $w \neq u \triangledown (u \triangledown w)$ *oder* $(c \otimes_{u,w} x) * y \in P$ *oder* $(c \otimes_{u,v} y) * x \in P$ *oder* $(c \otimes_{u,w} x) * y \neq (c \otimes_{u,v} y) * x$ *für* u, v, w *paarweise verschieden,* $(c,u),(x,w),(y,v) \in P \times V$

g) $u \triangledown w = v$ *oder* $u \triangledown v = w$ *oder* $(u \triangledown w) \triangledown v \neq (u \triangledown v) \triangledown w$ *oder* $(c \otimes_{u,w} x) \otimes_{u \triangledown w, v} y \neq (c \otimes_{u,v} y) \otimes_{u \triangledown v, w} x$ *für* u, v, w *paarweise verschieden,* $(c,u),(x,w),(y,v) \in P \times V$

Beweis Wir nehmen an, es gelte $(c \cdot x) \cdot y = (c \cdot y) \cdot x$ und untersuchen die verschiedenen Fälle für x, y und c.

- Fall $x, y \in S$:
  - $c \in S$

$$\begin{array}{rrcll} & (c \cdot x) \cdot y & = & (c * x) * y & = \\ & (c \cdot y) \cdot x & = & (c * y) * x & \\ \overset{a)}{\Leftrightarrow} & x & = & y & \end{array}$$

  - $(c,u) \in P \times V$

$$\begin{array}{rrcll} & ((c,u) \cdot x) \cdot y & = & (c * x, u) \cdot y & \\ & & = & ((c * x) * y, u) & = \\ & ((c,u) \cdot y) \cdot x & = & (c * y, u) \cdot x & \\ & & = & ((c * y) * x, u) & \\ \Leftrightarrow & (c * x) * y & = & (c * y) * x & \\ \overset{a)}{\Leftrightarrow} & x & = & y & \end{array}$$

- Fall $x \in S$, $(y,v) \in P \times V$ oder umgekehrt
  - $c \in S$

$$\begin{array}{rrcll} & (c \cdot x) \cdot (y,v) & = & (c * x) \cdot (y,v) & \\ & & = & ((c * x) * y, v) & = \\ & (c \cdot (y,v)) \cdot x & = & (c * y, v) \cdot x & \\ & & = & ((c * y) * x, v) & \\ \Leftrightarrow & (c * x) * y & = & (c * y) * x & \\ \overset{a)}{\Leftrightarrow} & x & = & y & \end{array}$$

    Widerspruch, denn $x \in S, y \notin S$.

– $(c,u) \in P \times V$, $u \neq v$

$$\begin{array}{rrcll} & ((c,u)\cdot x)\cdot(y,v) & = & (c*x,u)\cdot(y,v) & \\ & & = & ((c*x)\otimes_{u,v} y, u \bigtriangledown v) & = \\ & ((c,u)\cdot(y,v))\cdot x & = & (c\otimes_{u,v} y, u\bigtriangledown v)\cdot x & \\ & & = & ((c\otimes_{u,v} y)*x, u\bigtriangledown v) & \\ \Leftrightarrow & (c*x)\otimes_{u,v} y & = & (c\otimes_{u,v} y)*x & \end{array}$$

Widerspruch zu b).

– $(c,v) \in P \times V$, $(c*x)*y, c*y \in S$

$$\begin{array}{rrcll} & ((c,v)\cdot x)\cdot(y,v) & = & (c*x,v)\cdot(y,v) & \\ & & = & (c*x)*y & = \\ & ((c,v)\cdot(y,v))\cdot x & = & (c*y)\cdot x & \\ & & = & (c*y)*x & \\ \Leftrightarrow & (c*x)*y & = & (c*y)*x & \\ \overset{a)}{\Leftrightarrow} & x & = & y & \end{array}$$

Widerspruch.

– $(c,v) \in P \times V$, $(c*x)*y \notin S$, $c*y \in S$

$$\begin{array}{rrcll} & ((c,v)\cdot x)\cdot(y,v) & = & (c*x,v)\cdot(y,v) & \\ & & = & ((c*x)*y,v) & = \\ & ((c,v)\cdot(y,v))\cdot x & = & (c*y)\cdot x & \\ & & = & (c*y)*x & \\ \Leftrightarrow & ((c*x)*y,v) & = & (c*y)*x & \end{array}$$

Widerspruch.

– $(c,v) \in P \times V$, $(c*x)*y \in S$, $c*y \notin S$

$$\begin{array}{rrcll} & ((c,v)\cdot x)\cdot(y,v) & = & (c*x,v)\cdot(y,v) & \\ & & = & (c*x)*y & = \\ & ((c,v)\cdot(y,v))\cdot x & = & (c*y,v)\cdot x & \\ & & = & ((c*y)*x,v) & \\ \Leftrightarrow & (c*x)*y & = & ((c*y)*x,v) & \end{array}$$

Widerspruch.

– $(c,v) \in P \times V$, $(c*x)*y, c*y \notin S$

$$
\begin{array}{rrcl}
 & ((c,v)\cdot x)\cdot(y,v) & = & (c*x,v)\cdot(y,v) \\
 & & = & ((c*x)*y,v) \quad = \\
 & ((c,v)\cdot(y,v))\cdot x & = & (c*y,v)\cdot x \\
 & & = & ((c*y)*x,v) \\
\Leftrightarrow & (c*x)*y & = & (c*y)*x \\
\overset{a)}{\Leftrightarrow} & x & = & y
\end{array}
$$

Widerspruch.

- Fall $(x,w),(y,w) \in P \times V$
  - $c \in S$, $(c*x)*y, (c*y)*x \in S$

$$
\begin{array}{rrcl}
 & (c\cdot(x,w))\cdot(y,w) & = & (c*x,w)\cdot(y,w) \\
 & & = & (c*x)*y \quad = \\
 & (c\cdot(y,w))\cdot(x,w) & = & (c*y,w)\cdot(x,w) \\
 & & = & (c*y)*x \\
\Leftrightarrow & (c*x)*y & = & (c*y)*x \\
\overset{a)}{\Leftrightarrow} & x & = & y \\
\Leftrightarrow & (x,w) & = & (y,w)
\end{array}
$$

  - $c \in S$, $(c*x)*y \notin S$, $(c*y)*x \in S$
    Analog zu oben folgt ein Widerspruch.
  - $c \in S$, $(c*x)*y \in S$, $(c*y)*x \notin S$
    Analog zu oben folgt ein Widerspruch.
  - $c \in S$, $(c*x)*y, (c*y)*x \notin S$
    Analog zu oben folgt $(x,w) = (y,w)$.
  - $(c,u) \in P \times V$, $u \neq w$
    Es ist $u \bigtriangledown w \neq w$, denn sonst folgt $u = w$ im Widerspruch zur Voraussetzung.

$$
\begin{array}{rrcl}
 & ((c,u)\cdot(x,w))\cdot(y,w) & = & (c \otimes_{u,w} x, u \bigtriangledown w)\cdot(y,w) \\
 & & = & ((c \otimes_{u,w} x) \otimes_{u\bigtriangledown w,w} y, (u \bigtriangledown w) \bigtriangledown w) \\
 & & = & \\
 & ((c,u)\cdot(y,w))\cdot(x,w) & = & (c \otimes_{u,w} y, u \bigtriangledown w)\cdot(x,w) \\
 & & = & ((c \otimes_{u,w} y) \otimes_{u\bigtriangledown w,w} x, (u \bigtriangledown w) \bigtriangledown w) \\
\Leftrightarrow & (c \otimes_{u,w} x) \otimes_{u\bigtriangledown w,w} y & = & (c \otimes_{u,w} y) \otimes_{u\bigtriangledown w,w} x \\
\overset{e)}{\Leftrightarrow} & x & = & y \\
\Leftrightarrow & (x,w) & = & (y,w)
\end{array}
$$

– $(c, w) \in P \times V$, $c * x, c * y \in S$

$$\begin{array}{rrcll} & ((c,w)\cdot(x,w))\cdot(y,w) & = & (c*x)\cdot(y,w) & \\ & & = & ((c*x)*y,w) & = \\ & ((c,w)\cdot(y,w))\cdot(x,w) & = & (c*y)\cdot(x,w) & \\ & & = & ((c*y)*x,w) & \\ \Leftrightarrow & (c*x)*y & = & (c*y)*x & \\ \overset{a)}{\Leftrightarrow} & x & = & y & \\ \Leftrightarrow & (x,w) & = & (y,w) & \end{array}$$

– $(c, w) \in P \times V$, $c * x, c * y \in S$ oder $\notin S$ (alle anderen Fälle)
Analog zu oben folgt entweder ein Widerspruch, $(c*x)*y = ((c*y)*x, w)$ bzw. $((c * x) * y, w) = (c * y) * x$, oder $(c * x) * y = (c * y) * x$ und damit $(x, w) = (y, w)$.

- Fall $(x, w), (y, v) \in P \times V$, $w \neq v$

– $c \in S$

$$\begin{array}{rrcll} & (c\cdot(x,w))\cdot(y,v) & = & (c*x,w)\cdot(y,v) & \\ & & = & ((c*x)\otimes_{w,v} y, w \bigtriangledown v) & = \\ & (c\cdot(y,v))\cdot(x,w) & = & (c*y,v)\cdot(x,w) & \\ & & = & ((c*y)\otimes_{v,w} x, v \bigtriangledown w) & \\ \Leftrightarrow & (c*x)\otimes_{w,v} y & = & (c*y)\otimes_{v,w} x & \text{und} \\ & w \bigtriangledown v & = & v \bigtriangledown w & \end{array}$$

Widerspruch zu *c)*.

– $(c, w) \in P \times V$, $c * x \in S$

$$\begin{array}{rrcll} & ((c,w)\cdot(x,w))\cdot(y,v) & = & (c*x)\cdot(y,v) & \\ & & = & ((c*x)*y,v) & = \\ & ((c,w)\cdot(y,v))\cdot(x,w) & = & (c\otimes_{w,v} y, w \bigtriangledown v)\cdot(x,w) & \\ & & = & ((c\otimes_{w,v} y)\otimes_{w\bigtriangledown v,w} x, (w \bigtriangledown v) \bigtriangledown w) & \\ \Leftrightarrow & (c*x)*y & = & (c\otimes_{w,v} y)\otimes_{w\bigtriangledown v,w} x & \text{und} \\ & v & = & (w \bigtriangledown v) \bigtriangledown w & \end{array}$$

Widerspruch zu *d)*.

– $(c, w) \in P \times V$, $c * x \notin S$

$$
\begin{array}{lrll}
 & ((c,w)\cdot(x,w))\cdot(y,v) & = & (c*x,w)\cdot(y,v) \\
 & & = & ((c*x)\otimes_{w,v} y, w \bigtriangledown v) \quad = \\
 & ((c,w)\cdot(y,v))\cdot(x,w) & = & (c\otimes_{w,v} y, w\bigtriangledown v)\cdot(x,w) \\
 & & = & ((c\otimes_{w,v} y)\otimes_{w\bigtriangledown v,w} x, (w\bigtriangledown v)\bigtriangledown w) \\
\Rightarrow & w\bigtriangledown v & = & (w\bigtriangledown v)\bigtriangledown w \\
 & & \overset{\bigtriangledown \text{ idemp.}}{=} & (w\bigtriangledown v)\bigtriangledown(w\bigtriangledown v) \\
\Leftrightarrow & w & = & w\bigtriangledown v \\
 & & \overset{\bigtriangledown \text{ idemp.}}{=} & w\bigtriangledown w \\
\Leftrightarrow & v & = & w
\end{array}
$$

Widerspruch.

- Fall $(x,w),(y,v),(c,u)\in P\times V$, u,v,w paarweise verschieden
  - $u\bigtriangledown w = v$ und $u\bigtriangledown v = w$, $(c\otimes_{u,w} x)*y, (c\otimes_{u,v} y)*x \in S$

$$
\begin{array}{lrll}
 & ((c,u)\cdot(x,w))\cdot(y,v) & = & (c\otimes_{u,w} x, u\bigtriangledown w)\cdot(y,v) \\
 & & = & (c\otimes_{u,w} x)*y \quad = \\
 & ((c,u)\cdot(y,v))\cdot(x,w) & = & (c\otimes_{u,v} y, u\bigtriangledown v)\cdot(x,w) \\
 & & = & (c\otimes_{u,v} y)*x \\
\Leftrightarrow & (c\otimes_{u,w} x)*y & = & (c\otimes_{u,v} y)*x
\end{array}
$$

    Widerspruch zu *f)*.

  - $u\bigtriangledown w = v$ und $u\bigtriangledown v = w$, $(c\otimes_{u,w} x)*y \in S$, $(c\otimes_{u,v} y)*x \notin S$.
    Analog zu oben folgt $(c\otimes_{u,w} x)*y = ((c\otimes_{u,v} y)*x, w)$. Widerspruch.
  - $u\bigtriangledown w = v$ und $u\bigtriangledown v = w$, $(c\otimes_{u,w} x)*y \notin S$, $(c\otimes_{u,v} y)*x \in S$.
    Analog zu oben folgt $((c\otimes_{u,w} x)*y, v) = (c\otimes_{u,v} y)*x$. Widerspruch.
  - $u\bigtriangledown w = v$ und $u\bigtriangledown v = w$, $(c\otimes_{u,w} x)*y, (c\otimes_{u,v} y)*x \notin S$.
    Es folgt $((c\otimes_{u,w} x)*y, v) = ((c\otimes_{u,v} y)*x, w)$ und damit $v = w$.
    Widerspruch.
  - $u\bigtriangledown w = v$, $u\bigtriangledown v \neq w$ und $(c\otimes_{u,w} x)*y \in S$

$$
\begin{array}{lrll}
 & ((c,u)\cdot(x,w))\cdot(y,v) & = & (c\otimes_{u,w} x, u\bigtriangledown w)\cdot(y,v) \\
 & & = & (c\otimes_{u,w} x)*y \quad = \\
 & ((c,u)\cdot(y,v))\cdot(x,w) & = & (c\otimes_{u,v} y, u\bigtriangledown v)\cdot(x,w) \\
 & & = & ((c\otimes_{u,v} y)\otimes_{u\bigtriangledown v,w} x, (u\bigtriangledown v)\bigtriangledown w) \\
\Leftrightarrow & (c\otimes_{u,w} x)*y & = & ((c\otimes_{u,v} y)\otimes_{u\bigtriangledown v,w} x, (u\bigtriangledown v)\bigtriangledown w)
\end{array}
$$

    Widerspruch.

– $u \bigtriangledown w = v$, $u \bigtriangledown v \neq w$ und $(c \otimes_{u,w} x) * y \notin S$

$$\begin{array}{rrcl}
 & ((c,u)\cdot(x,w))\cdot(y,v) & = & (c \otimes_{u,w} x, u \bigtriangledown w)\cdot(y,v) \\
 & & = & ((c \otimes_{u,w} x) * y, u \bigtriangledown w) \quad = \\
 & ((c,u)\cdot(y,v))\cdot(x,w) & = & (c \otimes_{u,v} y, u \bigtriangledown v)\cdot(x,w) \\
 & & = & ((c \otimes_{u,v} y) \otimes_{u\bigtriangledown v,w} x, (u \bigtriangledown v) \bigtriangledown w) \\
\Rightarrow & u \bigtriangledown w & = & (u \bigtriangledown v) \bigtriangledown w \\
\Leftrightarrow & u & = & u \bigtriangledown v \\
\Leftrightarrow & u & = & v
\end{array}$$

Widerspruch.

– $u \bigtriangledown w \neq v$ und $u \bigtriangledown v \neq w$

$$\begin{array}{rrcl}
 & ((c,u)\cdot(x,w))\cdot(y,v) & = & (c \otimes_{u,w} x, u \bigtriangledown w)\cdot(y,v) \\
 & & = & ((c \otimes_{u,w} x) \otimes_{u\bigtriangledown w,v} y, (u \bigtriangledown w) \bigtriangledown v) \\
 & & = & \\
 & ((c,u)\cdot(y,v))\cdot(x,w) & = & (c \otimes_{u,v} y, u \bigtriangledown v)\cdot(x,w) \\
 & & = & ((c \otimes_{u,v} y) \otimes_{u\bigtriangledown v,w} x, (u \bigtriangledown v) \bigtriangledown w) \\
\Leftrightarrow & (c \otimes_{u,w} x) \otimes_{u\bigtriangledown w,v} y & = & (c \otimes_{u,v} y) \otimes_{u\bigtriangledown v,w} x \quad \text{und} \\
 & (u \bigtriangledown w) \bigtriangledown v & = & (u \bigtriangledown v) \bigtriangledown w
\end{array}$$

Widerspruch zu *g)*.

Damit haben wir gezeigt, dass $(S \cup (P \times V), \cdot)$ eine WTA-Quasigruppe ist. □

Beispiel 5.4 *Sei $(Q, *)$ ein total anti-symmetrischer Links-Loop (d.h. $0 * x = x$) mit gerader Ordnung $n+1$ und es gelte $x * 0 = (x)_n + 1$, $x * (x * 0) = 0$ für $x > 0$, dann existiert für alle ungeraden $m \leq n$ eine total anti-symmetrische Quasigruppe der Ordnung $mn + 1$.*

Beweis Wir definieren $u \bigtriangledown v := \frac{u+v}{2}$ auf $V := \mathbb{Z}_m$ und $S := \{0\}$. Auf der Menge $P = Q \backslash \{0\}$ definieren wir die Operationen $\otimes_{u,v}$ durch $x \otimes_{u,v} y := (-x - y + 2u + v)_n + 1$ mit Rechnung in $\mathbb{Z}_n$. Damit sind die Bedingungen von Lemma 5.14 erfüllt, im Einzelnen:

- Bed. *a)*: nach Voraussetzung
- Bed. *b)*: Es sei $x = 0$, $(c,u),(y,v) \in P \times V$ und $u \neq v$. Wir nehmen $(c * 0) \otimes_{u,v} y = (c \otimes_{u,v} y) * 0$ an,

$$\begin{array}{rrcll} & (c*0)\otimes_{u,v} y & = & (-(c)_n - 1 - y + 2u + v)_n + 1 & = \\ & (c\otimes_{u,v} y)*0 & = & (-c - y + 2u + v + 1)_n + 1 & \\ \Leftrightarrow & -c - 1 - y + 2u + v & =_n & -c - y + 2u + v + 1 & \\ \Leftrightarrow & 0 & =_n & 2. & \end{array}$$

Widerspruch.

- Bed. *c)*: Es gilt $v \bigtriangledown w = w \bigtriangledown v$, daher müssen wir $(0*x)\otimes_{w,v} y \neq (0*y)\otimes_{v,w} x$ für $v \neq w$ zeigen. Wir nehmen Gleichheit an, also

$$\begin{array}{rrcll} & (0*x)\otimes_{w,v} y & = & (-x - y + 2w + v)_n + 1 & = \\ & (0*y)\otimes_{v,w} x & = & (-y - x + 2v + w)_n + 1 & \\ \Leftrightarrow & -x - y + 2w + v & =_n & -y - x + 2v + w & \\ \Leftrightarrow & w & =_n & v. & \end{array}$$

  Da $m \leq n$, folgt auch $w =_m v$ im Widerspruch zu $w \neq v$.

- Bed. *d)*: Es sei $v = (w \bigtriangledown v) \bigtriangledown w = \frac{\frac{w+v}{2}+w}{2} \Leftrightarrow 3v = 3w$. Ist $\gcd(3, m) = 1$, dann folgt $v = w$ im Widerspruch zur Voraussetzung, falls nicht, dann müssen wir für $c, x, y > 0$ beweisen: $c * x = 0 \Rightarrow (c * x) * y \neq (c \otimes_{w,v} y) \otimes_{w \bigtriangledown v, w} x$. Sei

$$\begin{array}{rrcl} & (c*x)*y & = & 0*y \\ & & = & y \quad = \\ & (c\otimes_{w,v} y)\otimes_{w\bigtriangledown v,w} x & = & (-(-c - y + 2w + v)_n \\ & & & \quad -1 - x + w + v + w)_n + 1 \\ & & = & (c + y - 2w - v - 1 \\ & & & \quad -x + 2w + v)_n + 1 \\ & & = & (c + y - 1 - x)_n + 1 \\ \Leftrightarrow & y & =_n & c + y - x \\ \Leftrightarrow & c & =_n & x. \end{array}$$

  Es folgt also

$$\begin{array}{rrcl} & c*x & = & x*x \quad = \\ & 0 & = & x*(x*0) \\ \Leftrightarrow & x & = & x*0 \\ & & = & (x)_n + 1 \\ \Leftrightarrow & x & =_n & x + 1 \\ \Leftrightarrow & 0 & =_n & 1. \end{array}$$

Widerspruch.

- Bed. *e)*: Es gilt für $c, x, y > 0$

$$\begin{array}{rrcll}
 & (c \otimes_{u,w} x) \otimes_{u \bigtriangledown w, w} y & = & (-(-c - x + 2u + w)_n & \\
 & & & \quad -1 - y + u + w + w)_n + 1 & = \\
 & (c \otimes_{u,w} y) \otimes_{u \bigtriangledown w, w} x & = & (-(-c - y + 2u + w)_n & \\
 & & & \quad -1 - x + u + w + w)_n + 1 & \\
\Leftrightarrow & c + x - 2u - w & & c + y - 2u - w & \\
 & -1 - y + u + 2w & =_n & -1 - x + u + 2w & \\
\Leftrightarrow & x - y & =_n & y - x & \\
\Leftrightarrow & 2x & =_n & 2y & \\
\Leftrightarrow & x & =_n & y &
\end{array}$$

- Bed. *f)*: Falls $\gcd(3, m) = 1$, dann ist der erste Teil der Bedingung erfüllt, denn $w = u \bigtriangledown (u \bigtriangledown w) = \frac{u + \frac{u+w}{2}}{2} \Leftrightarrow 3u = 3w \Leftrightarrow u = w$. Andernfalls nehmen wir an: $(c \otimes_{u,w} x) * y = 0 = (c \otimes_{u,v} y) * x$ für u, v, w paarweise verschieden. Aus $x * ((x)_n + 1) = 0$ folgt

$$\begin{array}{rrcll}
 & y = (c \otimes_{u,w} x)_n + 1 & = & (-c - x + 2u + w + 1)_n + 1 & \text{und} \\
 & x = (c \otimes_{u,v} y)_n + 1 & = & (-c - y + 2u + v + 1)_n + 1 & \\
 & & = & (-c - (-c - x + 2u + w + 2) & \\
 & & & +2u + v + 1)_n + 1 & \\
 & & = & (-c + c + x - 2u - w - 2 & \\
 & & & +2u + v + 1)_n + 1 & \\
 & & = & (x - w - 1 + v)_n + 1 & \\
\Leftrightarrow & x & =_n & x - w + v & \\
\Leftrightarrow & w & =_n & v. &
\end{array}$$

Widerspruch.

- Bed. *g)*: Es sei $(u \bigtriangledown w) \bigtriangledown v = (u \bigtriangledown v) \bigtriangledown w$ bzw. $\frac{u+w}{2} + v = \frac{u+v}{2} + w$. Es folgt $u + w + 2v = u + v + 2w$ und damit $v = w$. Damit haben wir gezeigt: $(u \bigtriangledown w) \bigtriangledown v \neq (u \bigtriangledown v) \bigtriangledown w$ für $v \neq w$. □

Beispiel Die Quasigruppe $(Q, \cdot'')$ von Beispiel 5.3 erfüllt die Bedingungen $x * 0 = (x)_n + 1$ und $x * (x * 0) = 0$ für $x > 0$. Es folgt die Existenz einer TA-Quasigruppe der Ordnung $3 \cdot 3 + 1 = 10$ (siehe Seite 44, Abbildung 4.9).

5.6 Total anti-symmetrische Designs

In diesem Abschnitt untersuchen wir die Möglichkeit, TA-Quasigruppen mit Hilfe von Designs zu konstruieren. Damit durch die PBD-Konstruktion aus idempotenten WTA-Quasigruppen wieder eine solche entsteht, darf das PBD nicht folgende Figur enthalten. Ein Design ohne diese A-Figur nennen wir total anti-symmetrisch.

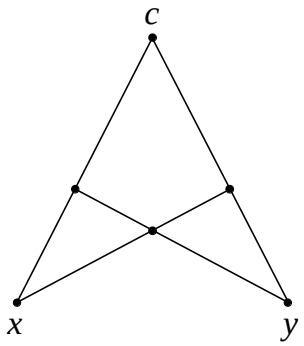

Abbildung 5.1: A-Figur

Damit gilt

Lemma 5.15 *Ist $S(2, K, v)$ ein total anti-symmetrisches Design und gibt es für alle $k \in K$ eine TA-Quasigruppe der Ordnung k, dann existiert eine TA-Quasigruppe der Ordnung v.*

Ein total anti-symmetrisches Design lässt sich mit einer distributiven Steiner Quasigruppe konstruieren.

Lemma 5.16 *Das zu einer distributiven Steiner-Quasigruppe gehörende Steinertripelsystem ist ein total anti-symmetrisches $S(2, 3, v)$.*

Beweis Sei $(Q, *)$ die distributive Steiner Quasigruppe und $S(2, 3, v)$ das zugehörige STS. Wir nehmen an, dass es in $S(2, 3, v)$ eine A-Figur mit den paarweise verschiedenen Punkten c, x, y gibt. Damit gilt dann $(c*x)*y = (c*y)*x$. $(Q, *)$ ist distributiv, wodurch $(c * x) * y = (c * y) * (x * y) = (c * y) * x$ folgt. Damit erhalten wir $x * y = x$ und $x = y$ im Widerspruch dazu, dass die Punkte verschieden sind. □

Die zu einem total anti-symmetrischen STS gehörende Steiner-Quasigruppe muss allerdings nicht zwingend distributiv sein. Dazu betrachten wir die folgenden

beiden Beispiele.

Beispiel Sei u ungerade. Auf der Punktmenge $P = \mathbb{Z}_u \times \mathbb{Z}_3$ definieren wir die Blöcke durch

$$\begin{aligned} B &= \{\{(i,0),(i,1),(i,2)\}|i \in \mathbb{Z}_u\} \cup \\ &\quad \{\{(a,j),(b,j),(\frac{a+b}{2},j+1)\}|a,b \in \mathbb{Z}_u, a \neq b, j \in \mathbb{Z}_3\}. \end{aligned}$$

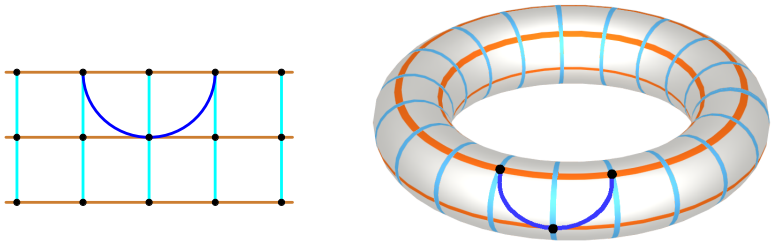

Abbildung 5.2: Total anti-symmetrisches Design

Für $u = 1,3,5,9,11,13,15,17,19$ erhält man mit dieser Konstruktion ein total anti-symmetrisches $S(2,3,u \cdot 3)$ und damit eine WTA-Quasigruppe der Ordnung $3 \cdot u$.

Für $u = 7$ ist das konstruierte Design nicht A-frei. In diesem Fall enthält es folgende Blöcke:

$$\begin{aligned} B_1 &= \{(0,0),(0,1),(0,2)\} \\ B_2 &= \{(0,0),(1,0),(4,1)\} \quad a = j = 0, b = 1 \\ B_3 &= \{(1,0),(0,2),(2,2)\} \quad a = 0, b = j = 2 \\ B_4 &= \{(0,1),(4,1),(2,2)\} \quad a = 0, b = 4, j = 1. \end{aligned}$$

Eine A-Figur wird durch die Punkte $c = (0,0)$, $x = (4,1)$, $y = (0,2)$ aufgespannt.

Für $u = 5$ ist die konstruierte Steiner-Quasigruppe nicht distributiv. Zum Beispiel ist $((0,0) * (1,0)) * (2,0) = (4,1) * (2,0) = (6,0) \neq ((0,0) * (2,0)) * ((1,0) * (2,0)) = (1,1) * (5,1) = (3,2)$.

Beispiel Eine ganz ähnliche Konstruktion stammt von Skolem 1927 ([5], Seite 317). Auf der Menge $\mathbb{Z}_u \times \mathbb{Z}_3$ wird ein STS definiert durch die Blöcke

$$\begin{aligned} B &= \{\{(i,0),(i,1),(i,2)\}|i \in \mathbb{Z}_u\} \cup \\ &\quad \{\{(a,j),(a+2b,j),(a+b,j+1)\}|a \in \mathbb{Z}_u, b = 1,\ldots,\frac{u-1}{2}, j \in \mathbb{Z}_3\}. \end{aligned}$$

Auch hier definiert dies ein total anti-symmetrisches Design, wenn $u = 1, 3, 5, 9, 11, 13, 15, 17, 19$ ist, wohingegen für $u = 7$ das Design eine A-Figur enthält. Mit $u = 5$ erhalten wir z. B. die folgende WTA-Quasigruppe der Ordnung 15:

$*$	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
00	00	02	01	10	06	14	04	12	11	13	03	08	07	09	05
01	02	01	00	12	11	07	09	05	13	06	14	04	03	08	10
02	01	00	02	08	13	09	14	10	03	05	07	12	11	04	06
03	10	12	08	03	05	04	13	09	02	07	00	14	01	06	11
04	06	11	13	05	04	03	00	14	10	12	08	01	09	02	07
05	14	07	09	04	03	05	11	01	12	02	13	06	08	10	00
06	04	09	14	13	00	11	06	08	07	01	12	05	10	03	02
07	12	05	10	09	14	01	08	07	06	03	02	13	00	11	04
08	11	13	03	02	10	12	07	06	08	14	04	00	05	01	09
09	13	06	05	07	12	02	01	03	14	09	11	10	04	00	08
10	03	14	07	00	08	13	12	02	04	11	10	09	06	05	01
11	08	04	12	14	01	06	05	13	00	10	09	11	02	07	03
12	07	03	11	01	09	08	10	00	05	04	06	02	12	14	13
13	09	08	04	06	02	10	03	11	01	00	05	07	14	13	12
14	05	10	06	11	07	00	02	04	09	08	01	03	13	12	14

Wie wir bereits gesehen haben, existiert ein STS nur für Ordnungen $n \equiv 1, 3 \mod 6$. Daher sind die beschriebenen Ansätze für Ordnungen $n = 4k + 2$ nicht anwendbar.

Die in der Literatur aufgeführten Designs (z.B. [5], [17]) werden häufig mit einer projektiven Ebene konstruiert. Eine projektive Ebene enthält allerdings immer eine A-Figur, weil sich zwei Geraden immer in einem Punkt schneiden. Die Frage, ob es total anti-symmetrische Designs mit $v = 4k + 2$ Punkten gibt, bleibt daher zunächst offen.

Kapitel 6

Existenz total anti-symmetrischer Quasigruppen

Ecker und Poch vermuteten 1986, dass es keine total anti-symmetrischen Quasigruppen der Ordnung $4k + 2$ gibt. Zunächst konnten wir die Vermutung stützen und zeigen (siehe Theorem 5.2), dass nahe liegende Ansätze nicht zum Erfolg führen können. Bereits Ende 1999 gelang es uns aber, per Computersuche (siehe nächstes Kapitel) TA-Quasigruppen der Ordnung 10 zu finden und somit die ersten Gegenbeispiele anzugeben. Knapp drei Jahre später folgten TA-Quasigruppen der Ordnung 14. Die Computersuche stößt, trotz optimierter Algorithmen, bei Ordnung 18 an ihre Grenzen, da die Anzahl der Quasigruppen mit der Ordnung stark anwächst (siehe [44]). Als nächstes entwickelten wir daher Konstruktionsmethoden für TA-Quasigruppen. Anfang 2003 hatten wir Konstruktionen für alle Ordnungen $n < 142$ und Ende 2003 konnten wir schließlich die Vermutung von Ecker und Poch vollständig widerlegen (mit Ausnahme natürlich der Fälle $n = 2, 6$) und zeigen:

Theorem 6.1 *Es existieren total anti-symmetrische Quasigruppen der Ordnung n für alle $n \neq 2, 6$.*

Beweis Während man total anti-symmetrische Quasigruppen für alle $n \neq 4k + 2$ recht leicht mit dem Galois-Körper $\mathrm{GF}(2^r)$ und dem Restklassenring $\mathbb{Z}_u$ konstruieren kann (Lemma 5.6), benötigen wir für $n = 4k + 2$ fast alle Konstruktionen aus dem vorherigen Kapitel. Eine grobe Übersicht über die benutzten Verfahren gibt das folgende Diagramm.

Den Beweis für $n = 4k + 2$ unterteilen wir in die drei Fälle $n \equiv 0, 1, 2 \mod 3$.

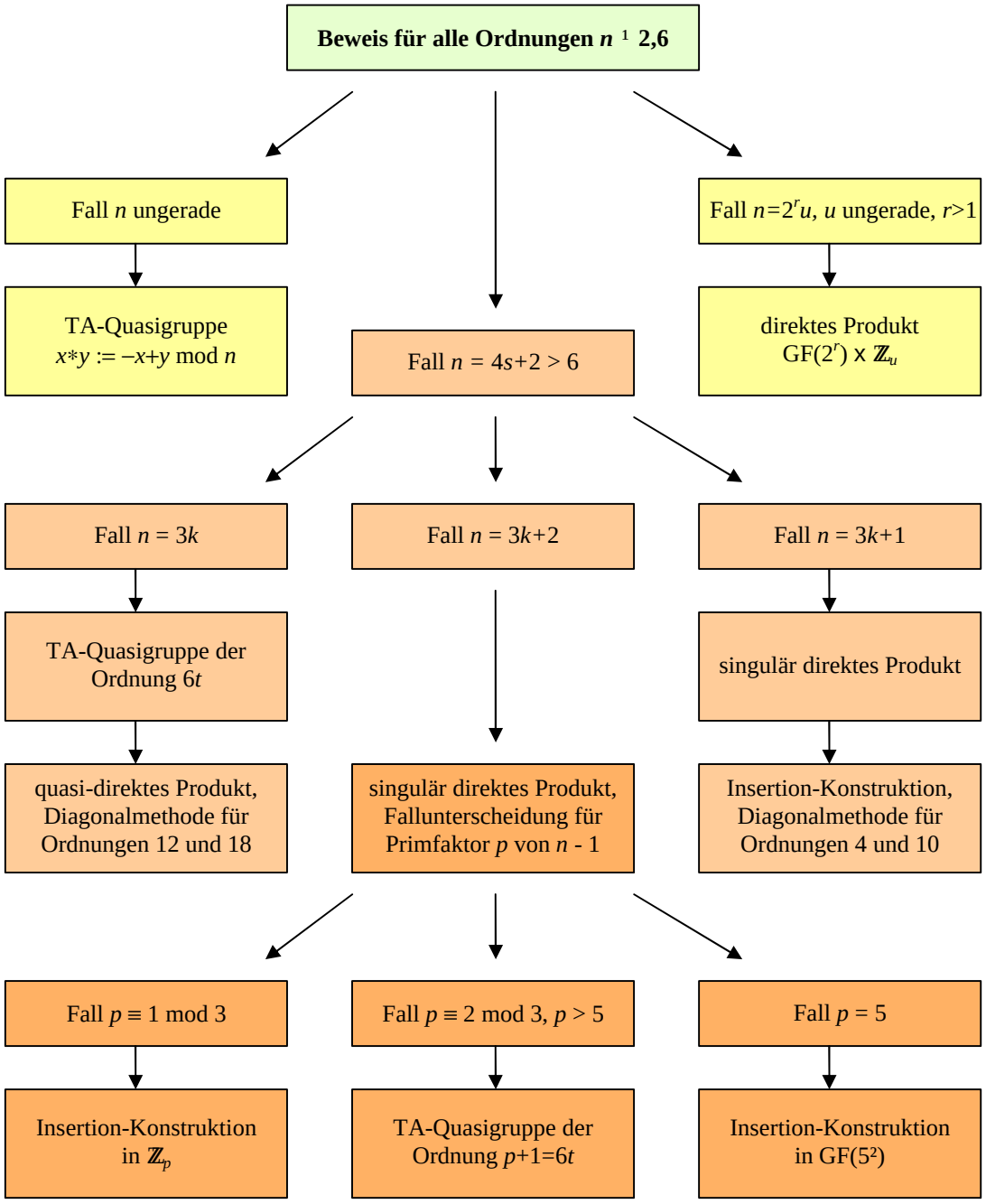

Abbildung 6.1: Beweisstruktur

6.1 Der Fall $n = 3k$

Gilt $n = 4s + 2 = 3k$, so ist n durch 2 und durch 3 teilbar, also auch durch 6. Für diesen Fall wenden wir das direkte und quasi-direkte Produkt im folgenden Lemma 6.2 an.

Um später das singulär direkte Produkt anwenden zu können, zeigen wir außerdem, dass die konstruierten TA-Quasigruppen die Bedingung $(x*0)*0 = x \Rightarrow x = 0$ erfüllen. Diese Anforderung ist auch der Grund dafür, dass wir diesen Fall nicht mit vollständiger Induktion beweisen: wenn wir annehmen, wir hätten eine TA-Quasigruppe $(Q, *)$ der Ordnung k und bilden das direkte Produkt mit der TA-Quasigruppe $(\mathbb{Z}_3, \cdot)$ der Ordnung 3

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

so gilt, wenn x der Fixpunkt der ersten Spalte $q_0 : x \mapsto x * 0$ von $(Q, *)$ ist (vgl. Lemma 7.2),

$$((x, 1) * (0, 0)) * (0, 0) = (x, 2) * (0, 0) = (x, 1).$$

Man kann sich leicht klarmachen, dass dies allgemein gilt: das Kreuzprodukt zweier TA-Quasigruppen der Ordnungen 3 und k erfüllt nie die Bedingung $(x * 0) * 0 = x \Rightarrow x = 0$.

Lemma 6.1 *Seien $(R, +, \cdot)$ ein kommutativer Ring mit Eins und $a - 1$, a, $a + 1$ Einheiten, dann existiert ein TA-Links-Loop der Ordnung $|R|$, für den $(x*0)*0 = x \Rightarrow x = 0$ gilt. Insbesondere ist das der Fall, wenn*

- *$R = \mathbb{Z}_u$ ist, u ungerade und nicht durch 3 teilbar, und*
- *$R = \mathrm{GF}(p^i)$, mit $p^i > 3$.*

Beweis Wir definieren $x * y := ax + y$, dann ist $(R, *)$ eine WTA-Quasigruppe. Wenn $(x*0)*0 = a^2x = x$ gilt, dann folgt $(a^2-1)x = (a-1)(a+1)x = 0$ und damit $x = 0$. Durch Umordung der Spalten erhalten wir den gesuchten TA-Links-Loop.

In $\mathbb{Z}_u$, u ungerade und nicht durch 3 teilbar, und in $\mathrm{GF}(p^i)$, $p \geq 5$, sind 1,2 und 3 Einheiten und wir setzen $a := 2$. In $\mathrm{GF}(2^i)$ bzw. $\mathrm{GF}(3^j)$, $i, j > 1$, sind 2 und 3 bzw. 3, 4 und 5 Einheiten und wir setzen $a := 2$ bzw. $a := 4$. □

Lemma 6.2 *Sei n durch 6 teilbar, $n > 6$, dann existiert ein TA-Links-Loop der Ordnung n, für den $(x * 0) * 0 = x \Rightarrow x = 0$ gilt.*

Beweis Sei $n = 2^i 3^j u$, u ungerade und nicht durch 3 teilbar, $i, j > 0$. Ist $u > 1$, so haben wir mit Lemma 6.1 einen TA-Links-Loop der Ordnung u mit $(x * 0) * 0 = x \Rightarrow x = 0$.

Fall 1: $i = j = 1$

Wir wählen $b_1 = 2$, $b_3 = 1$, $b_2 = 16$, dann sind $b_1, b_2, b_3, b_1 + b_3 = 3, b_1 - b_3 = 1, a_1 - 1 = -1/2, a_2 - 1 = 1, a_2 + 1 = 3$ Einheiten in $\mathbb{Z}_u$ und $a_1 = 1/2 \neq -1$. Damit sind die Voraussetzungen von Lemma 5.13 erfüllt und es folgt die Existenz eines TA-Links-Loops der Ordnung $n = 6u$.

Fall 2: $i = 1$, $j > 1$

Für Ordnung 18 erfüllt der folgende TA-Links-Loop die geforderte Bedingung (vgl. Seite 71).

$*$	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
00	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
01	02	03	00	04	07	09	12	01	16	14	17	08	05	11	06	10	15	13
02	03	14	04	00	05	08	10	13	02	17	15	01	09	06	12	07	11	16
03	04	17	15	05	00	06	09	11	14	03	01	16	02	10	07	13	08	12
04	05	13	01	16	06	00	07	10	12	15	04	02	17	03	11	08	14	09
05	06	10	14	02	17	07	00	08	11	13	16	05	03	01	04	12	09	15
06	07	16	11	15	03	01	08	00	09	12	14	17	06	04	02	05	13	10
07	08	11	17	12	16	04	02	09	00	10	13	15	01	07	05	03	06	14
08	09	15	12	01	13	17	05	03	10	00	11	14	16	02	08	06	04	07
09	10	08	16	13	02	14	01	06	04	11	00	12	15	17	03	09	07	05
10	11	06	09	17	14	03	15	02	07	05	12	00	13	16	01	04	10	08
11	12	09	07	10	01	15	04	16	03	08	06	13	00	14	17	02	05	11
12	13	12	10	08	11	02	16	05	17	04	09	07	14	00	15	01	03	06
13	14	07	13	11	09	12	03	17	06	01	05	10	08	15	00	16	02	04
14	15	05	08	14	12	10	13	04	01	07	02	06	11	09	16	00	17	03
15	16	04	06	09	15	13	11	14	05	02	08	03	07	12	10	17	00	01
16	17	02	05	07	10	16	14	12	15	06	03	09	04	08	13	11	01	00
17	01	00	03	06	08	11	17	15	13	16	07	04	10	05	09	14	12	02

In GF(9) dargestellt mit den Ziffern $0, 1, \ldots, 8$, sind $b_1 = 1$, $b_3 = 3$, $b_2 = 4$, $b_1 + b_3 = 4, b_1 - b_3 = 7, a_1 - 1 = 3 - 1 = 5, a_2 - 1 = 8 - 1 = 7, a_2 + 1 = 8 + 1 = 6$ Einheiten und $a_1 = 3 \neq 2 = -1$ (vgl. [32]). Damit sind die Voraussetzungen von Lemma 5.13 erfüllt und es folgt die Existenz eines TA-Links-Loops der Ordnung $n = 6 \cdot 9 = 54$ mit der gewünschten Bedingung.

Mit Lemma 6.1 haben wir einen TA-Links-Loop der Ordnung 9 mit $(x * 0) * 0 = x \Rightarrow x = 0$.

Ist nun $j = 2k + 1 > 3$, also $n = 54 \cdot 3^{2k-2} \cdot u = 54 \cdot 9^{k-1} \cdot u$, oder $j = 2k > 2$, also $n = 18 \cdot 3^{2k-2} \cdot u = 18 \cdot 9^{k-1} \cdot u$, so haben wir für jeden Faktor einen

TA-Links-Loop mit $(x * 0) * 0 = x \Rightarrow x = 0$ und durch das Kreuzprodukt damit auch für Ordnung n.

Fall 3: $i > 1$, $j = 1$

Analog zum vorherigen Fall, wobei wir aber statt GF(9) den Körper GF(4) benutzen. Für Ordnung 12 erfüllt der folgende TA-Links-Loop, konstruiert mit der Diagonalmethode, die geforderte Bedingung.

$*$	00	01	02	03	04	05	06	07	08	09	10	11
00	00	01	02	03	04	05	06	07	08	09	10	11
01	02	09	00	01	08	07	05	03	11	10	04	06
02	03	07	10	00	02	09	08	06	04	01	11	05
03	04	06	08	11	00	03	10	09	07	05	02	01
04	05	02	07	09	01	00	04	11	10	08	06	03
05	06	04	03	08	10	02	00	05	01	11	09	07
06	07	08	05	04	09	11	03	00	06	02	01	10
07	08	11	09	06	05	10	01	04	00	07	03	02
08	09	03	01	10	07	06	11	02	05	00	08	04
09	10	05	04	02	11	08	07	01	03	06	00	09
10	11	10	06	05	03	01	09	08	02	04	07	00
11	01	00	11	07	06	04	02	10	09	03	05	08

In GF(4) dargestellt mit den Ziffern $0, 1, 2, 3$, sind $b_1 = 1$, $b_3 = 2$, $b_2 = 3$, $b_1 + b_3 = 3, b_1 - b_3 = 3, a_1 - 1 = 2 - 1 = 3, a_2 - 1 = 2 - 1 = 3, a_2 + 1 = 2 + 1 = 3$ Einheiten und $a_1 = 2 \neq 1 = -1$. Damit sind die Voraussetzungen von Lemma 5.13 erfüllt und es folgt die Existenz eines TA-Links-Loops der Ordnung $n = 6 \cdot 4 = 24$ mit der gewünschten Bedingung.

Mit Lemma 6.1 haben wir einen TA-Links-Loop der Ordnung 4 mit $(x * 0) * 0 = x \Rightarrow x = 0$.

Ist nun $i = 2k + 1 > 3$, also $n = 24 \cdot 2^{2k-2} \cdot u = 24 \cdot 4^{k-1} \cdot u$, oder $i = 2k > 2$, also $n = 12 \cdot 2^{2k-2} \cdot u = 12 \cdot 4^{k-1} \cdot u$, so haben wir für jeden Faktor einen TA-Links-Loop mit $(x * 0) * 0 = x \Rightarrow x = 0$ und durch das Kreuzprodukt damit auch für Ordnung n.

Fall 4: $i, j > 1$

Mit Lemma 6.1 erhalten wir jeweils einen TA-Links-Loop der Ordnungen 2^i, 3^j und u mit $(x * 0) * 0 = x \Rightarrow x = 0$ und damit auch für $n = 2^i 3^j u$.

Damit haben wir alle Möglichkeiten abgedeckt. □

6.2 Der Fall $n = 3k + 1$

Wir benötigen zunächst eine TA-Quasigruppe mit bestimmten Eigenschaften.

Lemma 6.3 *Sei $n = 3^k u$ ungerade, u nicht durch 3 teilbar und $k \neq 1$. Dann existiert eine Quasigruppe $(D, \bigtriangledown)$ der Ordnung n mit folgenden Eigenschaften:*

1. $x \bigtriangledown x = x$, $(D, \bigtriangledown)$ *ist idempotent*
2. $x \bigtriangledown y = y \bigtriangledown x \Rightarrow x = y$
3. $(u \bigtriangledown w) \bigtriangledown v = (u \bigtriangledown v) \bigtriangledown w \Rightarrow v = w$, $(D, \bigtriangledown)$ *ist total anti-symmetrisch*
4. $w = u \bigtriangledown (u \bigtriangledown w) \Rightarrow u = w$
5. $v = (w \bigtriangledown v) \bigtriangledown w \Rightarrow v = w$

Beweis Da das Kreuzprodukt zweier solcher Quasigruppen wieder dieselben Eigenschaften hat, brauchen wir die Aussage nur für n prim, n nicht durch 3 teilbar und für $n = 3^k$, $k > 1$ zu zeigen.

Wir definieren $x * y = (1 - a)x + ay$ auf $\mathbb{Z}_p$, wobei a und $a - 1$ Einheiten sind. Damit gilt $x * x = (1 - a)x + ax = x - ax + ax = x$ und die erste Eigenschaft ist erfüllt. Wir nehmen an, dass $2a - 1$ eine Einheit ist, dann haben wir bei der zweiten Eigenschaft

$$\begin{array}{rrcll} & x \bigtriangledown y & = & (1-a)x + ay & = \\ & y \bigtriangledown x & = & (1-a)y + ax & \\ \Leftrightarrow & x - ax + ay & = & y - ay + ax & \\ \Leftrightarrow & (2a-1)x & = & (2a-1)y & \\ \Leftrightarrow & x & = & y. & \end{array}$$

Die dritte Eigenschaft ist ebenfalls erfüllt:

$$\begin{array}{rrcll} & (u \bigtriangledown w) \bigtriangledown v & = & (1-a)((1-a)u + aw) + av & \\ & & = & (1-a)^2 u + (1-a)aw + av & = \\ & (u \bigtriangledown v) \bigtriangledown w & = & (1-a)((1-a)u + av) + aw & \\ & & = & (1-a)^2 u + (1-a)av + aw & = \\ \Leftrightarrow & aw - a^2 w + av & = & av - a^2 v + aw & \\ \Leftrightarrow & -a^2 w & = & -a^2 v & \\ \Leftrightarrow & w & = & v & \end{array}$$

Damit die vierte Eigenschaft erfüllt wird, muss $a + 1$ eine Einheit sein:

$$\begin{aligned} & & w &= (1-a)u + a((1-a)u + aw) \\ & & &= (1-a)u + a(1-a)u + a^2 w \\ & & &= u - au + au - a^2 u + a^2 w \\ \Leftrightarrow & a^2 u - u &= a^2 w - w \\ \Leftrightarrow & (a^2-1)u &= (a^2-1)w \\ \Leftrightarrow & (a-1)(a+1)u &= (a-1)(a+1)w \\ \Leftrightarrow & u &= w \end{aligned}$$

Zuletzt prüfen wir noch die fünfte Eigenschaft. Hier benötigen wir, dass a^2-a+1 eine Einheit ist:

$$\begin{aligned} & & v &= (1-a)((1-a)w + av) + aw \\ & & &= (1-a)^2 w + (1-a)av + aw \\ \Leftrightarrow & (a^2-a+1)v &= (a^2-a+1)w \\ \Leftrightarrow & v &= w \end{aligned}$$

Ist $p > 3$ eine Primzahl, so wählen wir $a = 2$, dann sind $a, a-1 = 1, 2a-1 = 3, a+1 = 3, a^2-a+1 = 3$ Einheiten in $\mathbb{Z}_p$ und damit ist $x * y = -x + 2y$ die gesuchte Quasigruppe.

Für $n = 3^k$, $k > 1$ führen wir die selbe Konstruktion in $\mathrm{GF}(3^k)$ durch. In diesem Fall benötigen wir ein $a \neq 0, 1, 2 = \frac{1}{2} = -1$. Es ist dann auch $a^2 - a + 1 \neq 0$, denn in $\mathrm{GF}(3^k)$ gilt $(a+1)(a+1) = a^2 + 2a + 1 = a^2 - a + 1 = 0 \Leftrightarrow a = -1$. Da $\mathrm{GF}(3^k)$ für $k > 1$ mindestens 9 Elemente enthält, gibt es ein $a \in \mathrm{GF}(3^k)$ mit $a \neq 0, 1, 2$. □

Lemma 6.4 *Sei $(Q, *)$ ein total anti-symmetrischer Links-Loop mit gerader Ordnung $n + 1$ und es gelte $(-(x * 0) + y)_n + 1 \neq ((-x + y)_n + 1) * 0$, für $x, y > 0$, dann existiert für alle ungeraden $m = 3^t u$ mit $t \neq 1$ eine total anti-symmetrische Quasigruppe der Ordnung $nm + 1$.*

Beweis Wir nehmen die Quasigruppe $(D, \bigtriangledown)$ von Lemma 6.3 mit $D = \mathbb{Z}_m$ und $S := \{0\}$. Auf der Menge $P = Q \backslash \{0\}$ definieren wir die Operationen $\otimes_{u,v}$ durch $x \otimes_{u,v} y := (-x + y)_n + 1$. Damit sind die Bedingungen von Lemma 5.14 erfüllt. □

Lemma 6.5 *Sei $(Q, *)$, $Q = \{0, 1, \ldots, n\}$, ein total anti-symmetrischer Links-Loop der geraden Ordnung $n + 1$, für den $(x * 0) * 0 = x \Rightarrow x = 0$ gilt. Für alle $m = 3^t u$, $t \neq 1$, u ungerade und nicht durch 3 teilbar, gibt es dann eine TA-Quasigruppe der Ordnung $nm + 1$.*

Beweis Durch Umbenennung der Elemente und gleichzeitige Vertauschung der Zeilen erhalten wir einen zu $(Q, *)$ isotopen TA-Links Loop $(Q, \cdot)$,

$$x \cdot y := \psi^{-1}(\psi(x) * y), \quad \psi \text{ geeignet},$$

für den die Spaltenpermutation $q_0 : x \mapsto x \cdot 0$ eine Darstellung mit l Zyklen

$$q_0 = (1 \;\; 2 \;\; \ldots \;\; k_1)(k_1+1 \;\; k_1+2 \;\; \ldots \;\; k_2)\ldots(k_{l-1}+1 \;\; k_{l-1}+2 \;\; \ldots \;\; k_l)$$

besitzt, wobei $0 = k_0 < k_1 < \ldots < k_l$ und $k_i - k_{i-1} > 2$.

Um dies zu verdeutlichen, betrachten wir folgendes Beispiel: hat $q_0' : x \mapsto x * 0$ die Darstellung $q_0' = (1 \;\; 5 \;\; 2)(3 \;\; 6 \;\; 4 \;\; 7)$, so setzen wir $\psi = (2 \;\; 5 \;\; 6 \;\; 4 \;\; 3)$, dann ist $q_0 = \psi^{-1} \circ q_0' \circ \psi = (1 \;\; 2 \;\; 3)(4 \;\; 5 \;\; 6 \;\; 7)$.

Die Behauptung ergibt sich nun mit dem singulär direkten Produkt bzw. Lemma 6.4. Wir zeigen $(-(x \cdot 0) + y)_n + 1 \neq ((-x + y)_n + 1) \cdot 0$ für $x, y > 0$. Es ist $x \cdot 0 = x + 1$, falls $x \neq k_i$ oder $x \cdot 0 = k_{i-1} + 1$ falls $x = k_i > 0$.

1. Fall: Sei $x \neq k_1, \ldots, k_l$, wir nehmen an

$$\begin{array}{rrcl} & (-(x \cdot 0) + y)_n + 1 & = & ((-x + y)_n + 1) \cdot 0 \\ \Leftrightarrow & (-x - 1 + y)_n + 1 & = & ((-x + y)_n + 1) \cdot 0 \end{array}$$

Falls $(-x + y)_n + 1 \neq k_i$, $i = 1, \ldots, l$, so folgt

$$\begin{array}{rrcl} & (-x - 1 + y)_n + 1 & =_{n+1} & (-x + y)_n + 2 \\ \Leftrightarrow & (-x - 1 + y)_n & =_{n+1} & (-x + y)_n + 1 \end{array}$$

Die linke Seite der Gleichung liegt zwischen 0 und $n-1$, die rechte zwischen 1 und n, also liegen beide Seiten zwischen 1 und $n-1$ und die Gleichung gilt auch in $\mathbb{Z}_n$. Damit folgt

$$\begin{array}{rrcl} & -x - 1 + y & =_n & -x + y + 1 \\ \Leftrightarrow & 0 & =_n & 2 \end{array}$$

Widerspruch.

Falls $(-x + y)_n + 1 = k_i > 0$ für ein $i > 0$, so folgt

$$\begin{array}{rrcl} & (-x - 1 + y)_n + 1 & =_{n+1} & k_{i-1} + 1 \\ \Leftrightarrow & (-x - 1 + y)_n & =_{n+1} & k_{i-1} \end{array}$$

Mit $-x =_n k_i - y - 1$ folgt

$$\begin{array}{rrcl} & (k_i - y - 1 - 1 + y)_n & =_{n+1} & k_{i-1} \\ \Leftrightarrow & (k_i - 2)_n & =_{n+1} & k_{i-1} \end{array}$$

Widerspruch zu $k_i - k_{i-1} > 2$.

2. Fall: Sei $x = k_i > 0$ für ein $i > 0$, wir nehmen an

$$\begin{array}{rrcl} & (-(x \cdot 0) + y)_n + 1 & = & ((-x + y)_n + 1) \cdot 0 \\ \Leftrightarrow & (-k_{i-1} - 1 + y)_n + 1 & = & ((-k_i + y)_n + 1) \cdot 0 \end{array}$$

Falls $(-k_i + y)_n + 1 \neq k_j$, $j = 1, \ldots, l$, so folgt

$$\begin{array}{rrcl} & (-k_{i-1} - 1 + y)_n + 1 & =_{n+1} & (-k_i + y)_n + 2 \\ \Leftrightarrow & (-k_{i-1} - 1 + y)_n & =_{n+1} & (-k_i + y)_n + 1 \\ \Rightarrow & -k_{i-1} - 1 + y & =_n & -k_i + y + 1 \\ \Leftrightarrow & k_i - k_{i-1} & =_n & 2 \end{array}$$

Widerspruch zu $k_i - k_{i-1} > 2$.

Falls $(-k_i + y)_n + 1 = k_j > 0$ für ein $j > 0$, so folgt $y =_n k_j + k_i - 1$ und

$$\begin{array}{rrcl} & (-k_{i-1} - 1 + y)_n + 1 & =_{n+1} & k_{j-1} + 1 \\ \Leftrightarrow & (-k_{i-1} - 1 + k_j + k_i - 1)_n & =_{n+1} & k_{j-1} \\ \Rightarrow & (k_i - k_{i-1}) + (k_j - k_{j-1}) & =_n & 2 \end{array}$$

Ist $k_i = k_j$, so folgt $2(k_i - k_{i-1}) =_n 2$ bzw. $k_i - k_{i-1} =_n 1$, Widerspruch. Ist $k_i \neq k_j$, so gilt $2 < (k_i - k_{i-1}) + (k_j - k_{j-1}) \leq n$ (die Summe der Zyklenlängen ist immer kleiner oder gleich der Ordnung von q_0), im Widerspruch zu $(k_i - k_{i-1}) + (k_j - k_{j-1}) =_n 2$. □

Mit der Insertion-Konstruktion bzw. der Diagonalmethode erhalten wir folgende TA-Links-Loops der Ordnungen 4 und 10 mit $(x * 0) * 0 = x \Rightarrow x = 0$:

$*_4$	0	1	2	3
0	0	1	2	3
1	2	3	0	1
2	3	2	1	0
3	1	0	3	2

und

$*_{10}$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	2	6	0	4	1	7	9	5	3	8
2	3	9	7	0	5	2	8	1	6	4
3	4	5	1	8	0	6	3	9	2	7
4	5	8	6	2	9	0	7	4	1	3
5	6	4	9	7	3	1	0	8	5	2
6	7	3	5	1	8	4	2	0	9	6
7	8	7	4	6	2	9	5	3	0	1
8	9	2	8	5	7	3	1	6	4	0
9	1	0	3	9	6	8	4	2	7	5

Sei $k = 3^t \cdot u$, u nicht durch 3 teilbar. Ist $t = 1$, so gilt $n = 9u + 1$ und wir können das singulär direkte Produkt (Lemma 6.5) mit $(\mathbb{Z}_{10}, *_{10})$ und $m = u$ anwenden. Ist $t \neq 1$, so wenden wir Lemma 6.5 mit $(\mathbb{Z}_4, *_4)$ und $m = k$ an.

6.3 Der Fall $n = 3k + 2$

Bei der Insertion-Konstruktion (Lemma 5.11) stellt sich die Frage, wann es in einem Ring ein Element a gibt, für das $a^2 - a + 1$ ein Nullteiler oder gleich 0 ist. Im Ring $\mathbb{Z}_p$, $p > 2$ prim, ist dies gleichbedeutend mit der Frage, ob die Gleichung

$$a^2 - a + 1 =_p 0$$

eine Lösung besitzt. Wir multiplizieren die Gleichung mit 4 und erhalten

$$4a^2 - 4a + 4 =_p (2a - 1)^2 + 3 =_p 0.$$

Diese Gleichung besitzt aber genau dann eine Lösung, wenn es ein Element $x \in \mathbb{Z}_p$ gibt mit $x^2 =_p -3$. Gibt es ein solches x, so nennen wir -3 ein *quadratisches Residuum* modulo p. Mit Hilfe des aus der Zahlentheorie bekannten Legendre-Symbols lässt sich nun leicht zeigen, dass -3 genau dann ein quadratisches Residuum modulo p ist, wenn $p \equiv 1 \mod 3$. Damit erhalten wir:

Lemma 6.6 *Sei $p \equiv 1 \mod 3$ prim oder $q \equiv 2 \mod 3$ prim, $q > 2$, dann existiert ein TA-Links-Loop der Ordnung $p + 1$ bzw. $q^2 + 1$ mit $(x \cdot 0) \cdot 0 = x \Rightarrow x = 0$.*

Beweis Sei $p \equiv 1 \mod 3$ prim, dann gibt es ein Element a in $\mathbb{Z}_p$ mit $a^2 - a + 1 =_p 0$ und $a \neq 0, 1, 2$. Ist $2a - 1 =_p 0$, dann folgt $4a^2 =_p 4a - 4$ bzw. $2a \cdot 2a =_p$

$2 \cdot 2a - 4$ und damit $1 =_p -2$, im Widerspruch zu $p \equiv 1 \mod 3$. Damit sind die Bedingungen von Lemma 5.11 erfüllt, d.h. wir erhalten aus $(\mathbb{Z}_n, *)$, $n := p$, mit $x*y := (ax+(1-a)y+1)_n$ mit der Insertion Konstruktion eine WTA-Quasigruppe $(\mathbb{Z}_{n+1}, \cdot)$ der Ordnung $p+1$. Damit ist für $x < n$

$$x \cdot n = n \cdot x = x * x = (ax + (1-a)x + 1)_n = (x+1)_n$$

und $n \cdot n = n$. Wir definieren nun eine zu $(\mathbb{Z}_{n+1}, \cdot)$ isotope WTA-Quasigruppe $x \odot y := \varphi(\varphi(x) \cdot \psi(y))$, vgl. Lemma 5.2, mit $\varphi := (0 \quad n)$ und $\psi(x) := (x-1)_{n+1}$. Dann gilt für $x > 0$

$$0 \odot x = \varphi(\varphi(0) \cdot \psi(x)) = \varphi(n \cdot \psi(x)) = \varphi((\psi(x)+1)_n) = \varphi((x)_n) = x$$

und

$$0 \odot 0 = \varphi(\varphi(0) \cdot \psi(0)) = \varphi(n \cdot n) = \varphi(n) = 0.$$

Weiterhin gilt für $0 < x < n$

$$x \odot 0 = \varphi(\varphi(x) \cdot \psi(0)) = \varphi(x \cdot n) = \varphi((x+1)_n) = x + 1$$

und

$$n \odot 0 = \varphi(\varphi(n) \cdot \psi(0)) = \varphi(0 \cdot n) = \varphi(1) = 1.$$

Also $(x \odot 0) \odot 0 = x \Rightarrow x = 0$.

Sei $q \equiv 2 \mod 3$ prim. In $\mathbb{Z}_q = \mathrm{GF}(q)$ gibt es kein Element x mit $x^2 - x + 1 =_q 0$. Wir erhalten $\mathrm{GF}(q^2)$, indem wir den Körper $\mathrm{GF}(q)$ um $\sqrt{-3}$ erweitern. In $\mathrm{GF}(q^2)$ gibt es damit ein Element a mit $a^2 - a + 1 = 0$ und $a, a-1, 2a-1, a-2 \neq 0$. Wir definieren $x * y := ax + (1-a)y + 1$ und erhalten damit per Prolongation die WTA-Quasigruppe $(\mathrm{GF}(q^2) \cup \{n\}, \cdot)$. Für diese gilt

$$x \cdot n = n \cdot x = x * x = ax + (1-a)x + 1 = x + 1$$

und $n \cdot n = n$. Sei $\varphi = (0 \quad \sqrt{-3} \quad 2\sqrt{-3} \quad 3\sqrt{-3} \quad \ldots \quad (q-1)\sqrt{-3} \quad n)$ und $x \odot y := \varphi(\varphi^{-1}(x) \cdot \psi(y))$ mit $\psi(y) := n \backslash \varphi^{-1}(y)$, dann ist $(\mathrm{GF}(q^2) \cup \{n\}, \odot)$ eine TA-Quasigruppe, denn es gilt:

$$0 \odot x = \varphi(\varphi^{-1}(0) \cdot \psi(x)) = \varphi(n \cdot (n \backslash \varphi^{-1}(x))) = \varphi(\varphi^{-1}(x)) = x$$

und $(c \odot x) \odot y = (c \odot y) \odot x \Rightarrow x = y$ mit Lemma 5.2.

Nun müssen wir noch zeigen, dass $(x \odot 0) \odot 0 = x \Rightarrow x = 0$ gilt. Dazu sei $x = a + b\sqrt{-3} \in \mathrm{GF}(q^2)$, $x > 0$.

Fall 1: $0 < a < q - 1$

$$\begin{aligned} x \odot 0 &= \varphi(\varphi^{-1}(x) \cdot \psi(0)) \\ &= \varphi(\varphi^{-1}(a + b\sqrt{-3}) \cdot n) \\ &= \varphi((a + b\sqrt{-3}) \cdot n) \\ &= \varphi((a+1) + b\sqrt{-3}) \\ &= (a+1) + b\sqrt{-3} \\ &= x + 1 \end{aligned}$$

Fall 2: $a = 0$

$$\begin{aligned} x \odot 0 &= \varphi(\varphi^{-1}(b\sqrt{-3}) \cdot n) \\ &= \varphi(((b-1)\sqrt{-3}) \cdot n) \\ &= \varphi((b-1)\sqrt{-3} + 1) \\ &= 1 + (b-1)\sqrt{-3} \end{aligned}$$

Fall 3: $a = q - 1$

$$\begin{aligned} x \odot 0 &= \varphi(\varphi^{-1}((q-1) + b\sqrt{-3}) \cdot n) \\ &= \varphi(((q-1) + b\sqrt{-3}) \cdot n) \\ &= \varphi(((q-1) + b\sqrt{-3}) + 1) \\ &= \varphi(b\sqrt{-3}) \\ &= (b+1)\sqrt{-3}, \text{ falls } b < q-1 \text{ oder } = n, \text{ falls } b = q-1 \end{aligned}$$

Außerdem gilt

$$\begin{aligned} n \odot 0 &= \varphi(\varphi^{-1}(n) \cdot n) \\ &= \varphi(((q-1)\sqrt{-3}) \cdot n) \\ &= \varphi((q-1)\sqrt{-3} + 1) \\ &= 1 + (q-1)\sqrt{-3}. \end{aligned}$$

Damit hat q_0 die Darstellung

$$\begin{aligned} q_0 = \; & (1 \quad 2 \quad \ldots \quad q-1 \quad \sqrt{-3}) \\ & (1+\sqrt{-3} \quad 2+\sqrt{-3} \quad \ldots \quad q-1+\sqrt{-3} \quad 2\sqrt{-3}) \\ & \ldots \\ & (1+(q-1)\sqrt{-3} \quad 2+(q-1)\sqrt{-3} \quad \ldots \quad q-1+(q-1)\sqrt{-3} \quad n) \end{aligned}$$

und für $q > 2$ gilt $(x \odot 0) \odot 0 = x \Rightarrow x = 0$. □

Wir zeigen nun abschließend die Existenz einer TA-Quasigruppe der Ordnung $n = 4s+2$, falls $n = 3k+2$ ist. Dazu sei $p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_l^{k_l}$ die Primfaktorenzerlegung von $n - 1$.

- Gibt es ein $p := p_i \equiv 1 \mod 3$, so können wir die Insertion-Konstruktion bei $\mathbb{Z}_p$ anwenden. Nach Lemma 6.6 haben wir einen TA-Links-Loop der Ordnung $p + 1$ mit $(x * 0) * 0 = x \Rightarrow x = 0$.

- Falls der erste Fall nicht zutrifft, so gilt $p_i \equiv 2 \mod 3$ für alle i, denn $n-1 = 3k+1$ ist nicht durch 3 teilbar. Gibt es ein $p := p_i > 5$, so ist $p+1$ gerade und durch 3, also auch durch 6 teilbar. Nach Lemma 6.2 (quasi-direktes Produkt) gibt es einen TA-Links-Loop der Ordnung $p+1$ mit $(x * 0) * 0 = x \Rightarrow x = 0$.

- Als letzte Möglichkeit bleibt der Fall, dass $n - 1 = 5^{k_1}$ ist. Dann ist $k_1 > 1$ und wir erhalten einen TA-Links-Loop der Ordnung $p + 1$, $p := 5^2$, der $(x * 0) * 0 = x \Rightarrow x = 0$ erfüllt mit Lemma 6.6 (Insertion-Konstruktion mit $\mathrm{GF}(5^2)$).

Sei nun $m := (n-1)/p$, dann ist m nicht durch 3 teilbar. Mit dem singulär direkten Produkt (Lemma 6.5) haben wir eine TA-Quasigruppe der Ordnung $pm + 1 = n$.

Damit ist die Behauptung bewiesen. □

Kapitel 7

Algorithmische Methoden

Selbst mit heutigen Computern ist es unmöglich, alle Quasigruppen z.B. der Ordnung 10 zu konstruieren und dann zu prüfen, ob sie total anti-symmetrisch sind. Mit einigen Verbesserungen (Lemma 7.1 und 7.2) ist es uns aber möglich, TA-Quasigruppen bis zur Ordnung 14 per Computersuche zu finden. Außerdem weisen wir nach, dass es keine TA-Quasigruppe der Ordnung 10 gibt, welche alle (Sprung-)Zwillingsfehler oder alle Sprung-Transpositionen erkennt.

Durch Umordnung der Spalten einer TA-Quasigruppe erhalten wir einen total anti-symmetrischen Links-Loop. Daher können wir uns bei der Suche auf Links-Loops beschränken.

In einer Isomorphie-Klasse sind entweder alle oder keine Quasigruppen total anti-symmetrisch. Daher ist eine weitere Vereinfachung, möglichst nur einen Repräsentanten einer Isomorphie-Klasse zu konstruieren. Dies erreichen wir näherungsweise durch das folgende Lemma. Dazu sei $Q = \{0, \ldots, n-1\}$ und wir nehmen die natürliche Reihenfolge $0 < 1 < 2 < \ldots < n-1$ der Elemente an. Die Addition führen wir in der Gruppe $(\mathbb{Z}, +)$ durch.

Lemma 7.1 *Ein total anti-symmetrischer Links-Loop ist isomorph zu einem total anti-symmetrischen Links-Loop $(Q, \cdot)$, für den*

$$1 \cdot x \leq x + 2, \qquad x = 0, \ldots, n-1$$

gilt.

Beweis Sei $(Q, *)$ eine total anti-symmetrische Quasigruppe mit Linkseins 0. Wir beweisen das Lemma mit vollständiger Induktion.

Falls $1*0 \leq 2$ ist (Bem.: in diesem Fall gilt $1*0 = 2$), dann ist nichts zu zeigen. Gilt $1*0 > 0+2 = 2$, dann definieren wir $\varphi(1*0) := 2$, $\varphi(2) := 1*0$ und $\varphi(x) := x$

sonst. Die Quasigruppe $(Q, \cdot)$ mit $x \cdot y := \varphi(\varphi(x) * \varphi(y))$ ist isomorph zu $(Q, *)$, da $\varphi^{-1} = \varphi$ gilt und es ist $1 \cdot 0 = \varphi(\varphi(1) * \varphi(0)) = \varphi(1 * 0) = 2 \leq 0 + 2$.

Nun sei $(Q, *)$ isomorph zu $(Q, *')$, und es gelte $1 *' x \leq x + 2$ für $0 \leq x \leq k < n - 3$. Ist $1 *' (k + 1) > k + 3$, dann setzen wir $\varphi(1 *' (k + 1)) := k + 3$, $\varphi(k + 3) := 1 *' (k + 1)$ und $\varphi(x) := x$ sonst. Damit erfüllt die Quasigruppe $(Q, \cdot)$ mit $x \cdot y := \varphi(\varphi(x) * \varphi(y))$ die gesuchte Bedingung, denn es gilt

$$1 \cdot x = \varphi(\varphi(1) *' \varphi(x)) = \varphi(1 *' x) = 1 *' x \leq x + 2, \qquad \text{für } 0 \leq x \leq k$$

und

$$1 \cdot (k + 1) = \varphi(\varphi(1) *' \varphi(k + 1)) = \varphi(1 *' (k + 1)) = k + 3 = (k + 1) + 2$$

und $(Q, \cdot)$ ist isomorph zu $(Q, *)$.

Da für $x \geq n - 3$ die Aussage $1 * x \leq x + 2$ trivial ist (denn schließlich ist $1 * x \leq n - 1$ für alle $x \in Q$), haben wir damit das Lemma bewiesen. □

Wir brauchen also nur solche Quasigruppen zu konstruieren, welche eine Linkseins besitzen und für die $1 * x \leq x + 2$ gilt.

Eine weitere wichtige Eigenschaft ist, dass die Spaltenpermutationen $q_i : x \mapsto x * i$ einer TA-Quasigruppe genau einen Fixpunkt besitzen.

Lemma 7.2 *Sei $(Q, *)$ eine TA-Quasigruppe der Ordnung n mit den Spaltenpermutationen q_i, $i = 0, \ldots, n - 1$, dann existiert für alle i genau ein $x_i \in Q$ mit $q_i(x_i) = x_i$.*

Beweis Wir haben bereits in Lemma 5.7 gezeigt, dass $\beta(x) = x \backslash x$ eine Permutation ist. Zu einem vorgegebenen i gibt es also auch ein j mit $j \backslash j = i$ und es gilt $j * i = j * (j \backslash j) = j$. Analog zum Beweis von Lemma 5.7 folgt, dass diese Lösung eindeutig ist. □

Bei der Suche müssen daher nur die Permutationen betrachtet werden, die genau einem Fixpunkt besitzen.

7.1 Algorithmus

Die Eigenschaften einer TA-Quasigruppe legen es nahe, die Konstruktion nach Spaltenpermutationen $q_0, \ldots, q_{n-1}$ der Quasigruppe durchzuführen. Um einen Links-Loop zu erhalten, wählen wir $q_i(0) := i$. Wir konstruieren nun Spaltenpermutationen mit folgenden Eigenschaften:

(a) $q_i(x) = q_j(x) \Rightarrow i = j$

(b) $q_i \circ q_j(x) = q_j \circ q_i(x) \Rightarrow i = j$

(c) $q_i(1) \leq q_i(0) + 2$, $i = 0, \ldots, n-1$

(d) q_i besitzt genau einen Fixpunkt, $i = 0, \ldots, n-1$

Eigenschaft a) stellt sicher, dass wir eine Quasigruppe erhalten. Eigenschaft b) garantiert, dass die Quasigruppe die Bedingung $(x*i)*j = (x*j)*i \Rightarrow i = j$ erfüllt. Die Eigenschaften c) und d) beschleunigen die Suche erheblich. Die Quasigruppe definieren wir durch: $x * y := q_y(x)$.

Die Spalten bestimmen wir mit einer Siebmethode. Dazu sei $A_i^{(j)}$ die Menge der möglichen Spaltenpermutationen im j-ten Schritt, in Spalte i. Wir führen nun folgende Schritte durch:

1. `Setze` $A_i^{(0)} := \{p \in S_n | p(0) = i$, `Bed. (c)+(d) für` $p\}$
2. `for` $j := 0$ `to` $n-2$
3. `Wähle ein` $q_j \in A_j^{(j)}$
4. `for` $i := j+1$ `to` $n-1$
5. $A_i^{(j+1)} := \{p \in A_i^{(j)} |$ `Bed. (a)+(b) für` p `und` $q_j\}$
6. `Falls` $A_i^{(j+1)} = \emptyset$ `dann Abbruch`
7. `Wähle ein` $q_{n-1} \in A_{n-1}^{(n-1)}$

Lemma 7.3 *Falls der Algorithmus nicht abbricht, dann definiert $x * y := q_y(x)$ eine total anti-symmetrische Quasigruppe der Ordnung n.*

Beweis 1. $x * y := q_y(x)$ ist eine Quasigruppe: $a * y = b * y \Leftrightarrow q_y(a) = q_y(b) \Rightarrow a = b$. Falls $x * a = x * b$, dann folgt $q_a(x) = q_b(x)$, o.B.d.A. $a \geq b$. Falls $a > b$ ist, dann folgt $q_a \in A_a^{(a)} \subseteq A_a^{(b+1)}$ und $q_b \in A_b^{(b)}$. In Schritt 5 wurde aber $A_a^{(b+1)}$ so definiert, dass $q_a(x) \neq q_b(x)$ im Widerspruch zur Annahme $a > b$. Demnach gilt $a = b$.
2. $x * y := q_y(x)$ ist total anti-symmetrisch: Es gelte $(c * x) * y = (c * y) * x$ bzw. $q_x \circ q_y(c) = q_y \circ q_x(c)$. Analog zu 1. folgt $x = y$. $\square$

Der Algorithmus erlaubt uns, die Anzahl der total anti-symmetrischen Links-Loops bis zur Ordnung 9 zu bestimmen. Außerdem konnten wir mehr als 40 Millionen total anti-symmetrische Quasigruppen der Ordnung 10 konstruieren.

Ord.	Anzahl der Links-Loops (siehe [44])	total anti-symmetrisch
2	1	0
3	2	1
4	24	2
5	1.344	18
6	1.128.960	0
7	12.198.297.600	4.800
8	2.697.818.265.354.240	116.640
9	15.224.734.061.278.915.461.120	222.634.440
10	2.750.892.211.809.148.994.633.229.926.400	$> 40.000.000$

Die folgende total anti-symmetrische Quasigruppe der Ordnung 10 ist ein Beispiel einer Quasigruppe, die wir mit dem Algorithmus gefunden haben:

$*$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	2	0	3	5	6	4	8	1	9	7
2	5	7	8	4	2	9	0	3	6	1
3	6	4	7	1	9	3	2	8	5	0
4	7	9	6	8	5	0	1	2	4	3
5	8	2	0	6	3	1	5	9	7	4
6	1	3	5	9	8	7	4	0	2	6
7	9	5	4	7	0	2	3	6	1	8
8	4	8	1	0	7	6	9	5	3	2
9	3	6	9	2	1	8	7	4	0	5

Außerdem konnten wir mehr als 1000 total anti-symmetrische Quasigruppen der Ordnung 14 finden. Ein Beispiel:

$*$	00	01	02	03	04	05	06	07	08	09	10	11	12	13
00	00	01	02	03	04	05	06	07	08	09	10	11	12	13
01	02	03	04	00	01	07	08	09	10	05	06	12	13	11
02	04	00	01	02	03	09	10	05	06	07	08	13	11	12
03	01	02	03	04	00	12	07	13	09	06	11	08	10	05
04	03	04	00	01	02	06	11	08	12	10	13	05	07	09
05	09	10	12	11	08	00	01	03	13	04	07	02	05	06
06	10	13	07	05	12	02	00	06	03	11	04	01	09	08
07	11	08	13	10	05	04	12	00	01	03	09	06	02	07
08	05	12	09	13	06	11	04	02	00	08	03	07	01	10
09	07	11	05	08	13	10	09	12	04	00	01	03	06	02
10	08	05	06	12	09	03	13	11	07	02	00	10	04	01
11	13	09	08	06	07	01	02	10	11	12	05	00	03	04
12	06	07	10	09	11	08	05	01	02	13	12	04	00	03
13	12	06	11	07	10	13	03	04	05	01	02	09	08	00

Wenn wir die weiteren Bedingungen (z.B. $q_i \circ q_i(x) = q_j \circ q_j(x) \Rightarrow i = j$ für Zwillingsfehler) für die anderen Fehlertypen ergänzen, dann ist der Algorithmus schnell genug, um die Anzahl der TA-Quasigruppen bis Ordnung 10 zu bestimmen, die eine der anderen wichtigen Fehlerarten erkennen können:

Ord.	total anti-symmetrisch	erkennen alle Sprung-Transpositionen	erkennen alle Zwillingsfehler	erkennen alle Sprung-Zwillingsfehler
2	0	0	0	0
3	1	0	0	1
4	2	2	2	2
5	18	12	12	6
6	0	0	0	0
7	4.800	480	480	600
8	116.640	1.440	11.520	1.440
9	222.634.440	15.120	60.480	824.040
10	$> 40.000.000$	0	0	0

Es gibt also keine TA-Quasigruppe der Ordnung 10, welche alle Sprung-Transpositionen oder alle (Sprung-)Zwillingsfehler erkennt.

Interessant ist die Beobachtung, dass es offensichtlich TA-Quasigruppen gibt, die alle Sprung-Zwillingsfehler, aber nicht alle Zwillingsfehler erkennen. Ein einfaches Beispiel lässt sich für ungerade Ordnungen angeben: Die TA-Quasigruppe $(\mathbb{Z}_n, *)$, n ungerade, mit $x * y := -x + y$ erkennt alle Sprung-Zwillingsfehler, während alle Zwillingsfehler unerkannt bleiben.

7.2 Parallelisierbarkeit und Rechenzeiten

Die Berechnungen im vorherigen Abschnitt wurden gleichzeitig auf 4 PCs mit insgesamt 6 Prozessoren mit Taktfrequenzen von 200 MHz bis 600 MHz durchgeführt. Dabei haben wir ausgenutzt, dass sich der vorgestellte Algorithmus leicht parallelisieren läßt. Falls z.B. $A_0^{(0)}$ 1800 Permutationen enthält, so kann Prozessor 1 die Permutationen im Bereich 1 bis 300 bearbeiten, Prozessor 2 die von 301 bis 600, usw.

Am aufwendigsten ist die Berechnung der Anzahl der TA-Links-Loops der Ordnung 9. Zunächst werden bei einer Rechenzeit von knapp 3 Wochen alle 1.266.690 TA-Links-Loops bestimmt, welche die Bedingung $1*x \leq x+2$ erfüllen. Als nächstes werden die 5852 Repräsentanten der Äquivalenzklassen berechnet, Rechenzeit ca. 10 Minuten. Nun können wir jeden Repräsentanten darauf prüfen, welche Fehlerarten er erkennt und wie viele verschiedene Links-Loops in seiner Klasse liegen. Die Gesamtanzahl der TA-Links-Loops der Ordnung 9, inkl. Auswertung der weiteren Fehlerarten, nimmt damit weitere 8 Stunden in Anspruch.

Dass es keine TA-Quasigruppe der Ordnung 10 gibt, welche alle Sprung-Transpositionen oder alle (Sprung-)Zwillingsfehler erkennt, wurde in knapp 6 Wochen Rechenzeit bestimmt. Dabei nahm jede Fehlerart ca. 2 Wochen in Anspruch. Die TA-Quasigruppen der Ordnung 10 fand das System über einen Zeitraum von mehreren Monaten. Dabei wählte ein Prozessor jeweils zufällig Permutationen $q_0 \in A_0^{(0)}$ und $q_1 \in A_1^{(1)}$ aus und berechnete alle möglichen TA-Links-Loops (falls vorhanden), die diese Spaltenpermutationen enthalten.

7.3 Diagonalmethode

In Lemma 5.12 benötigen wir eine Permutation $p : \mathbb{Z}_n \to \mathbb{Z}_n$ mit folgenden Eigenschaften:

a) $p(0) \neq 0$

b) $p(x) - p(y) = x - y$ impliziert $x = y$

c) $p(y - p(x)) + p(x) = p(x - p(y)) + p(y)$ impliziert $x = y$

d) $x \neq p(0)$ und $x \neq -p(0)$ und $p(-p(0) + x) - p(-p(0) - x) = x$ impliziert $x = 0$

e) $p(x) \neq 0$ und $p(-p(x)) + p(x) = x + p(0)$ impliziert $x = 0$

f) $p(x) \neq 0$ und $p(x) \neq x$ und $p(p(x)) = x$ impliziert $x = 0$

Auch hier benutzen wir einen Back-Tracking-Algorithmus, um eine solche Permutation zu finden. Wir beginnen mit der Definition $p(0) := 1$ und streichen 1 aus den Mengen A_i der möglichen Zahlen an Position i, $i > 0$. An der nächsten Position j wählen wir eine noch nicht gestrichene Zahl $p_j \in A_j$ aus, setzen $p(j) := p_j$ und streichen diese wiederum aus A_i, $i > j$. Dabei prüfen wir, ob die Bedingung b) verletzt wird. Ist dies der Fall, so gehen wir einen Schritt zurück. Haben wir $p(x)$ für alle $x \in \mathbb{Z}_n$ definiert, prüfen wir die verbliebenen Bedingungen c) bis f).

Während bis $n < 20$ die Rechenzeit bis zum Finden der ersten Lösung unter einer Sekunde bleibt, steigt sie für größere n schlagartig an. Um Lösungen bis einschließlich $n = 27$ finden zu können, schränken wir den Suchraum ein, indem wir die ersten k Stellen einer Lösung für die Ordnung $n - 2$ übernehmen. Für $n = 27$ haben wir z.B. die $k = 8$ Stellen einer Lösung für Ordnung 25 übernommen.

Beispiel Hier einige Permutationen p, welche die benötigten Bedingungen erfüllen.

Ordnung 9:

$$p = (0\ 1\ 3\ 6\ 2)(4\ 8\ 5) \quad \text{und} \quad p = (0\ 1\ 3\ 8\ 7\ 4\ 2\ 6)$$

Ordnung 11:

$$p = (0\ 1\ 7\ 5\ 4)(2\ 10\ 3\ 6\ 8)$$

Ordnung 15:

$$p = (0\ 1)(3\ 7\ 12\ 9)(4\ 6\ 13\ 11)(5\ 8\ 14\ 10)$$

Ordnung 17:

$$p = (0\ 1)(3\ 5\ 15\ 10\ 6\ 9\ 13\ 7\ 4\ 11\ 16\ 8\ 14\ 12)$$

Ordnung 25:

$$p = (0\ 1)(3\ 5\ 9\ 18\ 8\ 24\ 17\ 15\ 20\ 12\ 23\ 6\ 13\ 19\ 14\ 11\ 21\ 10\ 22\ 16\ 4\ 7)$$

Ordnung 27:

$$p = (0\ 1)(3\ 5\ 9\ 20\ 11\ 24\ 17\ 4\ 7)(6\ 13\ 25\ 8)(10\ 26\ 14\ 19\ 16\ 22\ 12\ 21\ 15\ 23\ 18)$$

7.4 Software

Der konstruktive Beweis für die Existenz total anti-symmetrischer Quasigruppen aus dem vorherigen Kapitel legt es nahe, die Konstruktionen mit dem Computer ausführen zu lassen. Da bei der Herleitung der theoretischen Ergebnisse bereits eine große Anzahl entsprechender Programme für die einzelnen Konstruktionsmethoden entstand, war dies auch recht einfach zu realisieren. Als Programmierumgebung haben wir Delphi 7 (siehe www.borland.com) gewählt, die Algorithmen und Konstruktionen wurden in Pascal realisiert.

Das Programm gibt für einen vorgegebenen Bereich die vom Beweis benutzte Konstruktionsmethode aus. Optional kann man die Konstruktion ausführen und die entsprechende TA-Quasigruppe ausgeben lassen. Eine weitere Option ermöglicht es, zu prüfen, ob die Konstruktion wirklich eine TA-Quasigruppe liefert.

Bei größeren Ordnungen (über 10.000) sollte man bedenken, dass allein die Quasigruppe mehrere hundert Megabyte Speicher belegt. Das Prüfen der TA-Quasigruppe ist daher nur für Ordnungen kleiner 10.000 freigegeben.

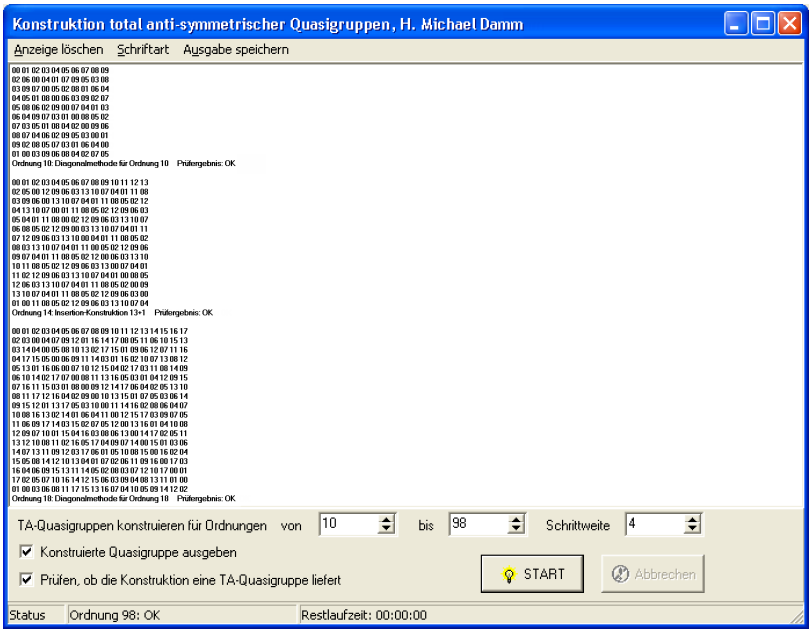

Abbildung 7.1: Konstruktion total anti-symmetrischer Quasigruppen

Ein zweites Programm implementiert den Algorithmus von Seite 105. Es ist für Ordnungen von 2 bis 10 ausgelegt und sucht nach total anti-symmetrischen Quasigruppen. Außerdem zeigt es an, wie viele TA-Quasigruppen zusätzlich alle Zwillingsfehler, Sprung-Zwillingsfehler, Sprung-Transpositionen und phonetischen Fehler erkennen.

Entfernt man das Häkchen bei „Bedingung $1 * x \leq x + 2$ erfüllt“ (vgl. Lemma 7.1), so prüft das Programm alle Permutationen und läuft entsprechend langsamer. Dies ermöglicht es uns aber, die Werte der Tabelle von Seite 107 direkt berechnen zu lassen. Wählen wir eine der Optionen „Nur TA-Quasigruppen suchen, die alle (Sprung-)Zwillingsfehler/Sprung-Transpositionen erkennen“, so können wir für Ordnung 10 nachweisen, dass es keine entsprechende TA-Quasigruppe gibt. Es sei aber angemerkt, dass es TA-Quasigruppen der Ordnung 10 gibt, die phonetische Fehler der Form $a0 \leftrightarrow 1a$, $a = 3, \ldots, 9$, erkennen (siehe Abbildung 7.2), d.h. sie erfüllen die Bedingung $(c * a) * 0 \neq (c * 1) * a$.

Da die systematische Suche aller TA-Quasigruppen der Ordnungen 9 und 10 zu lange dauern würde, wählt das Programm in diesen beiden Fällen die erste Spalte bzw. die ersten beiden Spalten der Quasigruppe zufällig aus. Dies geschieht allerdings nur, wenn keine Einschränkung auf bestimmte Fehlerarten gewählt ist.

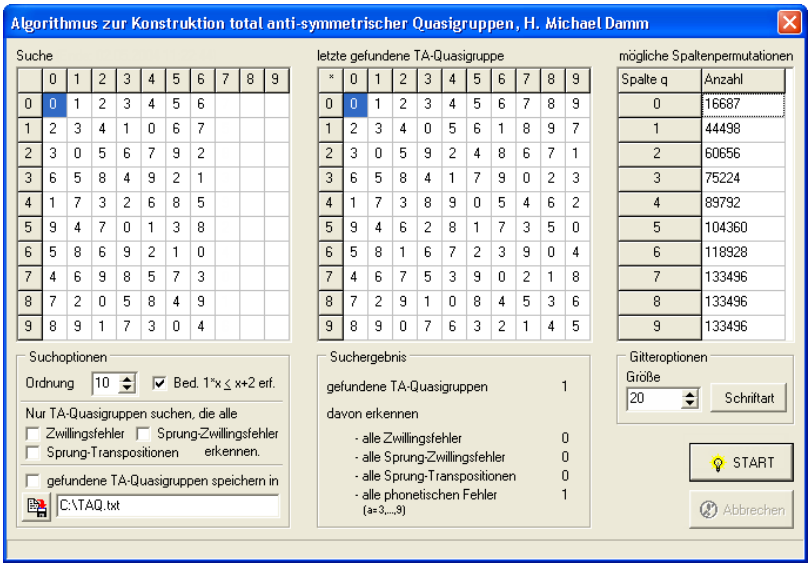

Abbildung 7.2: Konstruktion mit dem Algorithmus

Kapitel 8

Ausblick

Wir konnten die Existenz von TA-Quasigruppen für alle Ordnungen $n \neq 2, 6$ nachweisen und per Computersuche zeigen, dass eine TA-Quasigruppe der Ordnung 10 nicht alle (Sprung-)Zwillingsfehler und/oder alle Sprung-Transpositionen erkennt. Daraus folgt, dass ein Prüfziffersystem der Ordnung 10, welches diese Fehler erkennen kann, mit mindestens 2 verschiedenen Quasigruppen konstruiert werden müsste, also z.B. die Form

$$f(d_m, d_{m-1}, \ldots, d_1) := (((\ldots(d_m *_1 d_{m-1}) *_2 \ldots) *_1 d_3) *_2 d_2) *_1 d_1$$

mit verschiedenen Quasigruppen $*_1, *_2$ besitzt. Die Existenz eines solchen Prüfziffersystems mit zwei Quasigruppen $*_1, *_2$ kann man recht leicht nachweisen. In [18] haben wir gezeigt, dass die Diedergruppe $(D_n, \cdot)$, $n > 2$ ungerade, einen antisymmetrischen Anti-Automorphismus ψ besitzt, d.h. ψ erfüllt die Bedingungen

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

und

$$\psi(x) \cdot y = \psi(y) \cdot x \quad \Rightarrow \quad x = y.$$

Wir definieren

$$x *_1 y := \psi(x) \cdot y \qquad \text{und} \qquad x *_2 y := y \cdot \psi(x)$$

und erhalten damit ein Prüfziffersystem zur Basis $2n$. Dieser Ansatz, die $*_1, *_2$ zu definieren, bringt uns aber nicht weiter, wie wir in [18] gezeigt haben, weil so auch keine der weiteren wichtigen Fehlerarten erkannt werden kann. Man müsste nach Quasigruppen $*_1, *_2$ suchen, die nicht zu einer Gruppe der Ordnung 10 isotop sind.

Die nächste Verallgemeinerung ist der Ansatz mit mehr als 2 verschiedenen Quasigruppen:

$$f(d_m, d_{m-1}, \ldots, d_1) := (\ldots(d_m *_{m-1} d_{m-1}) *_{m-2} \ldots) *_1 d_1.$$

Eine interessante Möglichkeit, die Quasigruppen $*_i$ zu definieren, stammt von Ecker und Poch. Dazu sei $(Q, *)$ eine Quasigruppe und τ eine Permutation der Menge Q. Die $*_i$ werden nun durch

$$x *_{m-1} y := \tau^m(x) * \tau^{m-1}(y) \qquad \text{und} \qquad x *_i y := x * \tau^i(y),$$

$i = 1, \ldots, m-2$, definiert. Ecker und Poch konnten auch eine entsprechende Quasigruppe und eine Permutation für die Ordnungen $4k+2$ angeben, so dass alle Einzelfehler und Nachbarvertauschungen erkannt werden. Dieser „Shift-Code“ erkennt aber ebenfalls keine der weiteren Fehlerarten und der zweite angegebene Shift-Code erkennt nicht alle Nachbarvertauschungen. Hier stellt sich die Frage, ob mit anderen Quasigruppen und Permutationen der Ordnung 10 weitere Fehlerarten erkannt werden können.

Vielversprechend ist auch die Möglichkeit, ein Prüfziffersystem mit einer nicht in binäre Quasigruppen zerlegbaren n-Quasigruppe zu definieren. Der erste in Frage kommende Fall sind die irreduziblen 3-Quasigruppen. Zum Beispiel ist die folgende 3-Quasigruppe $f(i, j, k)$ der Ordnung 6 irreduzibel und anti-symmetrisch (siehe [18]):

$k =$	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5
j=0	0 1 2 3 4 5	1 2 0 5 3 4	2 0 1 4 5 3	3 4 5 1 2 0	4 5 3 0 1 2	5 3 4 2 0 1
1	2 0 1 4 5 3	0 1 2 3 4 5	1 2 0 5 3 4	5 3 4 2 0 1	3 4 5 1 2 0	4 5 3 0 1 2
2	1 2 0 5 3 4	2 0 1 4 5 3	0 1 2 3 4 5	4 5 3 0 1 2	5 3 4 2 0 1	3 4 5 1 2 0
3	4 5 3 0 1 2	3 4 5 1 2 0	5 3 4 2 0 1	0 1 2 4 5 3	2 0 1 5 3 4	1 2 0 3 4 5
4	5 3 4 2 0 1	4 5 3 0 1 2	3 4 5 1 2 0	1 2 0 3 4 5	0 1 2 4 5 3	2 0 1 5 3 4
5	3 4 5 1 2 0	5 3 4 2 0 1	4 5 3 0 1 2	2 0 1 5 3 4	1 2 0 3 4 5	0 1 2 4 5 3
	i=0	1	2	3	4	5

Per Computersuche könnte man versuchen, eine entsprechende anti-symmetrische 3-Quasigruppe der Ordnung 10 zu finden, welche eine der weiteren Fehlerarten erkennt. Oder man entwickelt Konstruktionen für irreduzible 3- bzw. n-Quasigruppen der Ordnung 10.

Danksagung

An dieser Stelle möchte ich Herrn Prof. Dr. H. P. Gumm für die freundliche Unterstützung bei der Ausarbeitung der vorliegenden Arbeit, Herrn Prof. Dr. R.-H. Schulz für wichtige Verbesserungsvorschläge und Herrn Prof. Dr. Bernhard Ganter für die Ideen zum Abschnitt „Total anti-symmetrische Designs“ danken. Mein weiterer Dank gilt Frau Petra Schulz für ihre Korrekturhilfe.

Literaturverzeichnis

[1] J. Aczél, V. D. Belousov, M. Hosszú. *Generalized assoziativity and bisymmetry on quasigroups*. Acta Math. Acad. Sci. Hungar 11 (1960), 127-136.

[2] R. D. Baker. *Quasigroups and tactical systems*. Aequationes Math. 18 (1978), 296-303.

[3] D. F. Beckley. *An optimum system with modulus* 11. The Comp. Bull. 11 (1967), 213-215.

[4] V. D. Belousov. *Uravnoveshennye tozhdestva v kvazigruppakh*. Mat. sbornik. 70 (1966), 55-97.

[5] Th. Beth, D. Jungnickel, H. Lenz. *Design Theory*. B.I.-Wissenschaftsverlag (1985).

[6] A. Beutelspacher. *Einführung in die endliche Geometrie I*. B.I.-Wissenschaftsverlag (1982).

[7] G. Birkhoff. *On the structure of abstract algebras*. Proc. Camb. Philos. Soc. 31 (1935), 433-454.

[8] G. Bol. *Gewebe und Gruppen*. Math. Ann. 114 (1937), 414-431.

[9] R. C. Bose, S. S. Shrikhande. *On the Falsity of Euler's Conjecture About the Non-existence of Two Orthogonal Latin Squares of Order* $4t + 2$. Proc. Natl. Acad. of Science 45 (1959), 734-737.

[10] R. C. Bose, S. S. Shrikhande. *On the Construction of Sets of Mutually Orthogonal Latin Squares and the Falsity of a Conjecture of Euler*. Trans. Amer. Math. Soc. 95 (1960), 191-209.

[11] R. C. Bose, S. S. Shrikhande, E. T. Parker. *Further Results on the Construction of Mutually Orthogonal Latin Squares and the Falsity of Euler's Conjecture*. Canad. J. Math. 12 (1960), 189-203.

[12] R. H. Bruck. *A Survey of Binary Systems*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 20, Springer-Verlag (1958).

[13] R. H. Bruck. *Simple quasigroups*. Bull. Amer. Math. Soc. 50 (1944), 769-781.

[14] R. H. Bruck. *Some results in the theory of quasigroups*. Trans. Amer. Math. Soc. 55 (1944), 19-52.

[15] S. Burris, H. P. Sankappanavar. *A Course in Universal Algebra*. Graduate Texts in Mathematics, Vol. 78 (1981). Millennium Edition Online: http://www.thoralf.uwaterloo.ca/htdocs/ualg.html

[16] O. Chein, H. O. Pflugfelder, J. D. H. Smith. *Quasigroups and Loops, Theory and Applications*. Sigma Series in Pure Mathematics, Volume 8 (1990), Heldermann Verlag Berlin.

[17] C. J. Colbourn, J. H. Dinitz. *The CRC handbook of combinatorial designs*. CRC Press Series on Discrete Mathematics and its Applications (1996).

[18] H. M. Damm. *Prüfziffersysteme über Quasigruppen*. Diplomarbeit Universität Marburg, März 1998.

[19] H. M. Damm. *Check digit systems over groups and anti-symmetric mappings*. Arch. Math. 75, No. 6 (2000), 413-421.

[20] H. M. Damm. *On the existence of totally anti-symmetric quasigroups of order* $4k + 2$. Computing 70, No. 4 (2003), 349-357.

[21] J. Dénes, A. D. Keedwell. *Latin Squares and their Applications*. New York: Academic Press (1974).

[22] J. Dénes, A. D. Keedwell. *Latin Squares - New Developments in the Theory and Applications*. Annals of discrete mathematics 46 (1991).

[23] DTA-Handbuch, http://www.sic.ch/de/dl_tkicch_dta.pdf

[24] A. Ecker, G. Poch. *Check Character Systems*. Computing 37 (1986), 277-301.

[25] T. Evans. *Universal Algebra and Euler's officer problem*. Amer. Math. Monthly 86 (1979), 466-473.

[26] O. Frink. *Symmetric and self-distributive systems*. Amer. Math. Monthly 62 (1955), 697-707.

[27] J. A. Gallian, M. Mullin. *Groups with Anti-symmetric Mappings*. Arch. Math. 65 (1995), 273-280.

[28] H. P. Gumm. *A New Class of Check-Digit Methods for Arbitrary Number Systems*. IEEE Trans. Inf. Th. 31 (1985), 102-105.

[29] H. P. Gumm. *Encoding of Numbers to Detect Typing Errors*. Intern. J. Applied Eng. Ed. 2 (1986), 61-65.

[30] M. Hall. *Projective planes*. Trans. Amer. Math. Soc. 54 (1943), 229-277.

[31] M. Hall, L. J. Paige. *Complete mappings of finite groups*. Pacific J. Math. 5 (1955), 541-549.

[32] A. Heiligenbrunner. *Online-Taschenrechner für endliche Körper*. http://members.aon.at/aheil/gf.htm.

[33] Th. Ihringer. *Allgemeine Algebra*. Berliner Studienreihe zur Mathematik (2003), Heldermann Verlag.

[34] K. W. Johnson, B. L. Sharma. *Constructions of weak inverse property loops*. Rocky Mointains J. of Math. 11 (1981), 1-8.

[35] T. P. Kirkman. *On a problem in combinations*. Cambridge and Dublin Math. J. 2 (1847), 191-204.

[36] J. Kirtland. *Identification numbers and check digit schemes*. Math. Assoc. of America. (2001).

[37] Z. Lie. *A Short Disproof of Euler's Conjecture Concerning Orthogonal Latin Squares*. Ars Comb. 14 (1982), 47-55.

[38] C. C. Lindner. *Construction of quasigroups satisfying the identity* $x(xy) = yx$. Can. Math. Bull. 14 (1971), 57-59.

[39] C. C. Lindner. *The generalized singular direct product for quasigroups*. Can. Math. Bull. 14 (1971), 61-63.

[40] C. C. Lindner. *Construction of quasigroups using the singular direct product*. Proc. Amer. Math. Soc. 29 (1971), 263-266.

[41] H. B. Mann. *The construction of orthogonal latin squares*. Ann. Math. Statistics 13 (1942), 418-423.

[42] H. B. Mann. *On Orthogonal Latin Squares*. Bull. Amer. Math. Soc. 50 (1944), 249-257.

[43] H. F. MacNeish. *Euler Squares*. Annals of Mathematics 23 (1923), 221-227.

[44] B. D. McKay, E. Rogoyski. *Latin Squares of Order 10*. Electronic J. of Comb. 2 (1995) #N3,
http://www.combinatorics.org/Volume_2/PDFFiles/v2i1n3.pdf

[45] T. Mituhisa. *Abstractions of symmetric functions*. Tôhoku Math. J. 49 (1943) 145-207.

[46] E. Netto. *Zur Theorie der Tripelsysteme*. Math. Ann. 42 (1893), 143-152.

[47] J. M. Osborn. *New loops from old geometries*. Amer. Math. Monthly 68 (1961), 103-107.

[48] E. T. Parker. *Construction of some sets of mutually orthogonal Latin squares*. Proc. Amer. Math. Soc. 10 (1959), 946-949.

[49] L. J. Paige. *A note on finite abelian groups*. Bull. Amer. Math. Soc. 53 (1947), 590-593.

[50] L. J. Paige. *Complete mappings of finite groups*. Pacific J. Math. 1 (1951), 111-116.

[51] M. J. Pelling, D. G. Rogers. *Stein quasigroups I: Combinatorial aspects*. Bull. Austral. Math. Soc. 18 (1978), 221-236.

[52] H. O. Pflugfelder. *Quasigroups and Loops, Introduction*. Sigma Series in Pure Mathematics, Volume 7 (1990), Heldermann Verlag Berlin.

[53] *Prüfziffernberechnung*. http://www.pruefziffernberechnung.de.

[54] A. Sade. *Groupoides automorphes par le groupe cyclique*. Can. J. Math. 9 (1957), 321-335.

[55] A. Sade. *Quasigroupes obéissant à certaines lois*. Rev. Fac. Sci. Univ. Istan., Ser. A 22 (1958), 151-180.

[56] A. Sade. *Produit direct singulier de quasigroups orthogonaux et anti-abéliens*. Ann. Soc. Sci. Bruxelles Ser. I, 74 (1960), 91-99.

[57] R.-H. Schulz. *Codierungstheorie. Eine Einführung*. Vieweg V. Braunschweig/Wiesbaden (2003), 2. Auflage.

[58] R.-H. Schulz. *A note on Check character Systems using Latin squares*. Discr. Math. 97 (1991) 371-375.

[59] R.-H. Schulz. *Check character systems over groups and orthogonal Latin squares*. Appl. Algebra Eng. Commun. Comput. 7 (1996), 125-132.

[60] M. Sholander. *On the existence of the inverse operation in alternation groupoids*. Bull. Amer. Math. Soc. 55 (1949), 746-757.

[61] H. Siemon. *Anwendungen der elementaren Gruppentheorie in Zahlentheorie und Kombinatorik*. Stuttgart: Klett-Verlag 1981.

[62] S. K. Stein. *On the foundations of quasigroups*. Trans. Amer. Math. Soc. 85 (1957), 228-256.

[63] J. Steiner. *Combinatorische Aufgabe*. J. reine angew. Math. 45 (1853), 181-182.

[64] D. R. Stinson. *A Short Proof of the Nonexistence of a Pair of Orthogonal Latin Squares of Order Six*. J. Comb. Theory, Ser. A, 36 (1984), 373-376.

[65] G. Tarry. *Le problème des 36 officiers*. C.R. Assoc. France Av. Sci. 29 (1900) 2, 170-203.

[66] J. Verhoeff. *Error detecting decimal codes*. Math. Centre Tracts 29, Amsterdam 1969.

[67] Die Welt. *Friedmann-Vermerk landete bei einem Pizzabäcker*. Artikel erschienen am 2. Juli 2003, http://www.welt.de/data/2003/07/02/127537.html

[68] R. L. Wilson. *Quasidirect products of quasigroups*. Commun. Algebra 3 (1975), 835-850.

[69] R. M. Wilson. *Constructions and uses of pairwise balanced designs*. Math. Centre Tracts 55 (1974), 18-41.

[70] K. Yamamoto. *Generation principles of latin squares*. Bull. Inst. Int. Stat. 38 (1961), 73-76.

Lebenslauf

Name	H. Michael Damm
Geburtsdatum	20. Oktober 1972
Geburtsort	Marburg-Wehrda
Eltern	Karl Damm, Elisabeth Damm (geb. Werner)

Schulbildung

1979 bis 1983	Grundschule Buchenau
1983 bis 1985	Mittelpunktschule Dautphetal
1985 bis 1992	Gymnasium Lahntalschule-Biedenkopf, Allgemeine Hochschulreife
1992	1. Preisträger in der ersten und zweiten Runde des Bundeswettbewerbs Mathematik

(Als dritter Sohn in der Familie wurde mein Antrag auf Nichtheranziehung zum Wehrdienst angenommen.)

Hochschulausbildung

1992 bis 1998	Mathematikstudium an der Universität Marburg
1997 bis 1998	Anfertigung der Diplomarbeit bei Prof. Dr. H. P. Gumm zum Thema „Prüfziffersysteme über Quasigruppen“
1998 bis 2004	Anfertigung der vorliegenden Dissertation bei Prof. Dr. H. P. Gumm

Berufliche Tätigkeit

seit 1993 freiberuflich tätig als Softwareentwickler u. a. für folgende Projekte:
- Portooptimierung von Infopostsendungen
- Ident- und Leitcodeerstellung für Frachtpost/Infopost Schwer
- Dublettensuche in Datenbanken
- Datenbankclient für ein Callcenter mit 200 Mitarbeitern
- Lagerverwaltung mit Anbindung von mobilen Datenterminals

Erklärung

Ich versichere, dass ich meine Dissertation selbstständig, ohne unerlaubte Hilfe angefertigt und mich dabei keiner anderen als der von mir ausdrücklich bezeichneten Quellen und Hilfen bedient habe.

Die Dissertation wurde in der jetzigen oder einer ähnlichen Form noch bei keiner anderen Hochschule eingereicht und hat noch keinen sonstigen Prüfungszwecken gedient.

Marburg, den 10. Mai 2004