# Perpendicular Arrays

## Diplomarbeit

Yves Edel
Werderstraße 29
6900 Heidelbeg

8.6.1993

# Inhaltsverzeichnis

# 1 Einführung

## 1.1 Begriffsklärung

In dieser Arbeit werden die behandelten kombinatorischen Objekte meist als Matrizen dargestellt. Wir werden eine Matrix A auch als eine Multimenge von Abbildungen ansehen. Hier ist die Urbildmenge die Menge K der Spalten, die Bildmenge ist die Menge V der Einträge und jede Zeile z von A liefert eine Abbildung $z : K \to V$. Sei jetzt A eine Matrix, S eine Menge von Spalten von A und T eine Menge von Einträgen von A. Häufig interessieren wir uns für Aussagen der Form: *Zu der Menge S von Spalten gibt es eine $\lambda$-Menge L von Zeilen von A, so daß für jede Zeile z aus L gilt: $z(S) \supseteq T$.* Wir führen die folgende abkürzende Schreibweise für diesen Sachverhalt ein: *In der Menge S von Spalten kommt die Menge T von Einträgen $\lambda$-mal vor.*

**(1.1) Definition** *Seien $\lambda,t,k,v \in \mathbb{N}$. Ein* Perpendicular Array *mit den Parametern $\lambda,t,k,v$ (kurz $PA_\lambda(t,k,v)$) ist eine k-spaltige Matrix A mit Einträgen aus einer v-Menge, so daß gilt:*

1. *Jede Zeile von A ist eine injektive Abbildung.*
2. *In jeder t-Menge von Spalten von A kommt jede (ungeordnete) t-Menge von Einträgen genau $\lambda$-mal vor.*

*Wir sprechen von einem PA(t,k,v), falls uns der Wert von $\lambda$ nicht interessiert. Ein $PA_\lambda(t,k,v)$ A heißt* induktiv, *falls gilt:*

- *Für alle $t' \leq t$ ist A ein PA(t',k,v).*

*Ein induktives $PA_\lambda(t,k,v)$ heißt ein* Authentication Perpendicular Array *(kurz $APA_\lambda(t,k,v)$) falls gilt:*

- *Für alle $t' \leq t$ und für jede t'-Menge U von Einträgen und jedes $u \in U$ gilt: In den Zeilen, die U enthalten, kommt U-{u} in jeder (t'-1)-Menge von Spalten gleich oft vor, unabhängig von u bzw. U.*

*Will man die v-Menge V der Einträge bzw. die k-Menge K der Spalten benennen, so schreibt man $PA_\lambda(t,k,V)$ bzw. $PA_\lambda(t,K,v)$.*

**(1.2) Beispiel**

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 |
| 1 | 2 | 3 | 4 | 0 |
| 2 | 3 | 4 | 0 | 1 |
| 3 | 4 | 0 | 1 | 2 |
| 4 | 0 | 1 | 2 | 3 |
| 0 | 2 | 4 | 1 | 3 |
| 2 | 4 | 1 | 3 | 0 |
| 4 | 1 | 3 | 0 | 2 |
| 1 | 3 | 0 | 2 | 4 |
| 3 | 0 | 2 | 4 | 1 |

Dies ist ein $PA_{10}(5,5,5)$. Es ist induktiv, da es auch ein $PA_2(4,5,5)$, ein $PA_1(3,5,5)$, ein $PA_1(2,5,5)$ und ein $PA_2(1,5,5)$ ist.

**(1.3) Beispiel**

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 4 |
| 3 | 4 | 1 |
| 4 | 1 | 2 |

Dies ist ein $PA_1(3,3,4)$, aber kein $PA(2,3,4)$, da z.B. in dem Spaltenpaar {1,2} die Menge {1,3} von Einträgen nicht vorkommt. Also ist dieses $PA_1(3,3,4)$ nicht induktiv.

**(1.4) Beispiel**

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 1 |
| 3 | 1 | 2 |
| 1 | 2 | 4 |
| 2 | 4 | 1 |
| 4 | 1 | 2 |
| 1 | 3 | 4 |
| 3 | 4 | 1 |
| 4 | 1 | 3 |
| 2 | 3 | 4 |
| 3 | 4 | 2 |
| 4 | 2 | 3 |

Dies ist ein $APA_3(3,3,4)$ somit auch ein $APA_2(2,3,4)$.

Die in dieser Arbeit benutzten kombinatorischen Strukturen seien hier zur Begriffsklärung definiert:

**(1.5) Definition** *Seien $\lambda,t,v \in \mathbb{N}$, $K \subseteq \mathbb{N}$. Ein* partially balanced Design *(kurz PBD) t-$(v,K,\lambda)$ besteht aus einer Teilmenge $\mathcal{B}$ der Potenzmenge einer v-Menge V, so daß gilt:*

1. *Für alle $B \in \mathcal{B}$ gilt $|B| \in K$.*
2. *Jede t-Menge aus V liegt in genau $\lambda$ Elementen $B \in \mathcal{B}$.*

*Ist $K=\{k\}$, so nennt man den PBD einen* Design *und schreibt t-$(v,k,\lambda)$ oder $S_\lambda(t,k,v)$.*
*Die Elemente $B \in \mathcal{B}$ nennt man die Blöcke des PBD.*

**(1.6) Definition** *Seien $\lambda,t,k,v \in \mathbb{N}$. Ein* Ordered Design *mit den Parametern $\lambda,t,k,v$ (kurz $OD_\lambda(t,k,v)$) ist eine k-spaltige Matrix A mit Einträgen aus einer v-Menge V, so daß gilt:*

1. *Jede Zeile von A ist eine injektive Abbildung.*
2. *In jeder t-Menge von Spalten kommt jedes (geordnete) t-Tupel von paarweise verschiedenen Einträgen genau $\lambda$ mal vor.*

**(1.7) Definition** *Seien $\lambda,t,k,v \in \mathbb{N}$. Ein* Orthogonal Array *mit den Parametern $\lambda,t,k,v$ (kurz $OA_\lambda(t,k,v)$) ist eine k-spaltige Matrix mit Einträgen aus einer v-Menge V, so daß gilt:*

- *In jeder t-Menge von Spalten kommt jedes (geordnete) t-Tupel von Einträgen genau $\lambda$ mal vor.*

**(1.8) Definition** *Ein* lateinisches Quadrat *der Ordnung v ist eine vxv-Matrix A mit Einträgen aus einer v-Menge, so daß gilt:*

1. *In jeder Zeile kommt jeder Eintrag genau einmal vor.*
2. *In jeder Spalte kommt jeder Eintrag genau einmal vor.*

*Zwei lateinische Quadrate $A=(a_{i,j})$ und $B=(b_{i,j})$ der Ordnung v heißen* orthogonal *wenn gilt:*

- *die geordneten Tupel $(a_{i,j},b_{i,j})$ sind alle verschieden.*

*Eine Kurzschreibweise für* paarweise orthogonale lateinische Quadrate *ist* MOLS.
*Man sagt, k paarweise orthogonale lateinische Quadrate der Ordnung v haben eine* gemeinsame Transversale, *falls gilt:*

- *Es gibt v Stellen d.h. Paare von Zeilen und Spalten $(i_l,j_l)$ l=1..v, so daß gilt:*
  - *die Zeilen $i_l$, l=1..v sind paarweise verschieden,*
  - *die Spalten $j_l$, l=1..v sind paarweise verschieden,*
  - *für jedes der k lateinischen Quadrate gilt: an diesen Stellen stehen alle v verschiedenen Einträge.*

**(1.9) Bemerkung**

*a)* *Ein $PA_1(1,v,v)$ ist äquivalent zu einem lateinischen Quadrat der Ordnung v.*

*b)* *Ein $OD_\lambda(t,k,v)$ ist ein $PA_{\lambda\, t!}(t,k,v)$.*

*c)* *Ein $PA_\lambda(t,k,v)$ ist ein Design t-$(v,k,\lambda\binom{k}{t})$.*

*d)* *Ein $OD_\lambda(2,k,v)$ läßt sich zu einem $OA_\lambda(2,k,v)$ ergänzen.*

*e)* *Ein $OA_1(2,k+2,v)$ ist äquivalent zu k paarweise orthogonalen lateinischen Quadraten der Ordnung v.*

*Beweis:* a,b und c ergeben sich unmittelbar aus den Definitionen.

d) Man ergänze das OD durch je $\lambda$ Kopien der Zeilen (i,...,i) für jeden der v Einträge i.

e) Man wähle zwei Spalten des OA aus, deren Einträge man als Koordinaten der Zeilen bzw. Spalten des zu konstruierenden lateinischen Quadrats interpretiere. Jede der restlichen Spalten liefert ein lateinisches Quadrat, indem man dem Eintrag einer Zeile in dieser Spalte als Eintrag des lateinischen Quadrats an den durch diese Zeile gegebenen Koordinaten benutzt. Die so erhaltenen lateinischen Quadrate sind paarweise orthogonal. Der Prozeß ist offensichtlich umkehrbar. ❑

**(1.10) Beispiel**

$$A:\begin{array}{cccc}1&2&3&4\\1&3&4&2\\1&4&2&3\\2&1&4&3\\4&1&3&2\\3&1&2&4\\3&4&1&2\\4&2&1&3\\2&3&1&4\\4&3&2&1\\3&2&4&1\\2&4&3&1\end{array}\qquad B:\begin{array}{cccc}1&2&3&4\\1&3&4&2\\1&4&2&3\\2&1&4&3\\4&1&3&2\\3&1&2&4\\3&4&1&2\\4&2&1&3\\2&3&1&4\\4&3&2&1\\3&2&4&1\\2&4&3&1\\1&1&1&1\\2&2&2&2\\3&3&3&3\\4&4&4&4\end{array}$$

$$LQ_1:\begin{array}{cccc}1&3&4&2\\4&2&1&3\\2&4&3&1\\3&1&2&4\end{array}\qquad LQ_2:\begin{array}{cccc}1&4&2&3\\3&2&4&1\\4&1&3&1\\2&3&1&4\end{array}$$

A ist ein $OD_1(2,4,4)$. B ist das gemäß (1.9 d) aus A gewonnene $OA_1(2,4,4)$. Indem man die beiden ersten Spalten von B als Koordinaten auffaßt erhält man nach (1.9 e) die beiden MOLS $LQ_1$ und $LQ_2$ .

## 1.2 Historischer Überblick

### 1.2.1 Rao's Arbeit

Soweit mir bekannt ist werden PA zum erstenmal im Artikel von Rao [21] aus dem Jahre 1961 untersucht. Dort werden PA als *orthogonal Arrays of Type II* und OD als *orthogonal Arrays of Type I* bezeichnet. Das Studium dieser Strukturen wird motiviert durch die Tatsache, daß sie Verallgemeinerungen von Objekten sind, die zur Konstruktion von paarweise orthogonalen lateinischen Quadraten verwendet wurden. Dies sind $OD_1(2,k,v)$ und $PA_1(2,k,v)$ die sich zu $OD_1(2,k,v)$ komplettieren lassen. Dazu einige Beispiele:

- In [22] wird ein $PA_1(2,5,15)$, auf dessen Einträgen eine Gruppe transitiv operiert, konstruiert. Dies liefert 4 MOLS der Ordnung 15.
- In [9] wird ein $OD_1(2,6,12)$, auf dessen Einträgen eine Gruppe transitiv operiert, konstruiert. Dies liefert 5 MOLS der Ordnung 12.
- In [31] wird ein spezielles $OD_1(2,4,14)$ konstruiert. Dies liefert 3 MOLS der Ordnung 14.

Die zugehörige Theorie wird in (3.10) behandelt.

Rao zeigt die folgenden Beziehungen zwischen $OD_1(2,k,v)$ und paarweise orthogonalen lateinischen Quadraten. Hier bedeutet das Symbol $A \Rightarrow B$, daß aus der Existenz des Objekts A die Existenz des Objekts B folgt.

**(1.11) Bemerkung** (Theorem 1 [21])

*(a)* $(k\text{-}1)$ *MOLS der Ordnung* $v \Rightarrow OD_1(2,k,v)$.

*(b)* $OD_1(2,k,v) \Rightarrow (k\text{-}2)$ *MOLS der Ordnung* $v$.

*(c)* $OA_1(2,k+1,v) \Rightarrow OD_1(2,k,v)$.

*(d) (k-2) MOLS der Ordnung v mit einer gemeinsamen Transversalen ⇔ $OD_1(2,k,v)$.*

*Beweis:*

(a)⇔(c) nach (1.9 e).

(b) $OD_1(2,k,v) \Rightarrow OA_1(2,k,v)$ (siehe (1.9 d)) und $OA_1(2,k,v) \Rightarrow$ (k-2) mols der Ordnung v (siehe (1.9 e)).

(c) Sei die v-Menge der Einträge ={1..v}. Permutiert man die Einträge einer Spalte eines OA, so erhält man wieder ein OA. Man kann also erreichen, daß v Zeilen des OA die Form (1i...i) $1 \le i \le v$ haben. Streicht man nun diese v Zeilen und die erste Spalte, so erhält man eine Matrix, die in jedem Spaltenpaar alle geordneten Paare verschiedener Einträge genau einmal enthält; also ein $OD_1(2,k,v)$.

(d) "⇐" Das in (b) mit (1.9 d) konstruierte OA hat v Zeilen der Form (i...i) $1 \le i \le v$ was äquivalent zu einer gemeinsamen Transversalen ist, denn an der Stelle (i,i) steht der Eintrag i.
"⇒" Nach (1.9 e) erhalten wir ein $OA_1$ (2,k,v). Da die lateinischen Quadrate eine gemeinsame Transversale haben, gibt es v Zeilen des OA, die in jeder Spalte v verschiedene Elemente stehen haben. Durch Permutieren der Einträge jeder Spalte erhält man v Zeilen der Form (i...i) $1 \le i \le v$. Streicht man diese v Zeilen, so erhält man ein $OD_1(2,k,v)$. ❑

Ferner hat Rao schon eine Konstruktion für $PA_1(2,q,q)$ gefunden, für jede ungerade Primzahlpotenz q (Theorem 2 [21]); dies wird in Kapitel 3 behandelt.

### 1.2.2 Spezielle Konstruktionen

Danach gab es eine Reihe von Arbeiten, die sich mit der Konstruktion von $PA_\lambda(t,k,v)$ befaßten, wobei das PA teilweise zusätzliche Eigenschaften zu erfüllen hat. In der ersten Phase wurden dann meist PA mit $\lambda=1$, $t=2$, $k=3,4,5$ für fast alle ungeraden v konstruiert. (Für $t=2$ und v gerade ist $\lambda$ notwendig gerade, wie wir im nächsten Kapitel sehen werden.) Teilweise wurden von diesen Autoren der Begriff des PA dadurch eingeschränkt, daß nur die Parameter $\lambda=1$, $t=2$ und daher auch nur ungerades v zugelassen wurden. Ich gebe hier nun eine kurze chronologische Übersicht über diese Arbeiten.

- In [20] werden konstruiert: $PA_1(2,3,v)$ für alle ungeraden $v \ge 3$, $PA_1(2,4,v)$ für alle ungeraden $v>3$, $v \ne 87$, und $PA_1(2,5,v)$ für alle ungeraden $v>3$, $v \notin \{33,39,51,87,219\}$.
- In [18] wird untersucht, welche Gruppen auf den Spalten eines $PA_1(2,k,v)$, $k=3,4,5$, operieren können. Diese PA werden dann bis auf einige Ausnahmen für alle ungeraden v konstruiert.
- In [17] wird untersucht, wann ein $OD_1(2,k,v)$ in zwei $PA_1(2,k,v)$ zerlegt werden kann, wobei vorausgesetzt wird, daß die PA durch Permutation ihrer Spalten auseinander hervorgehen. Diese PA werden dann, wieder einmal nur für $k=3,4,5$ und fast alle ungeraden v, konstruiert.
- In [15] werden $PA_3(3,4,v)$ konstruiert. Diese sind aber nicht induktiv und sind deshalb für Anwendung weniger geeignet. (vgl. im Gegensatz Bsp.(2.24. 2))

In den folgenden Arbeiten wird ein neuer Blickwinkel auf PA erschlossen. In Kapitel 4 wird dieser Aspekt vorgestellt.

- In [19] wird gezeigt, daß die folgenden Objekte äquivalent sind: ein $PA_1(2,5,v)$, auf dessen Spalten eine Gruppe der Ordnung 5 operiert, und eine speziellen Partition der Kanten des vollständigen Graphen $K_v$ auf v Ecken in Kreise der Länge 5. Eine solche Struktur kann nur existieren, wenn $v \equiv 1,5 \pmod{10}$ ist. Alle solche PA werden konstruiert mit Ausnahme des Falles v=15, wo kein solches existiert.

  [23], [10] und [16] liefern weitere Ergebnisse dieser Art.

Neue Bedeutung erlangten die PA, als Stinson ihre Verwendbarkeit in der Kryptographie entdeckte:[25],[26] und die wichtigste Arbeit in dieser Richtung: [27]. Diese führte dann auch zur Einführung der APA und zu ersten Konstruktionen derselben.

In den nachfolgenden Arbeiten beschäftigte man sich dann mit der Konstruktion von APA:

- In [28] werden einige APA mit t=3 und t=4 aus t-homogenen Gruppen gewonnen.
- In [7] werden $APA_\lambda(2,2^f+1,2^f+1)$ durch Halbierung der Gruppe $PGL_2(2^f)$ für ungerades f gewonnen.
- In [32] werden neue rekursive Konstruktionen entwickelt, die aus vorhandenen APA neue APA liefern.
- In [8] werden ein $APA_2(2,6,6)$ und ein $APA_3(3,9,9)$ gefunden und darauf basierende APA konstruiert.

Die Beschreibung der Verwendung der induktiven PA und der APA in der Kryptographie wird am Ende des nächsten Kapitels geliefert, da wir dann die notwendigen Begriffe haben, um die Anwendung für die Authentikation in etwas größerer Allgemeinheit darstellen zu können.

Um im folgenden einen übersichtlichen Aufbau der Theorie der PA zu erreichen, verzichte ich darauf, die Ergebnisse aus der Literatur chronologisch abzuhandeln. Da sich die Theorie oft allgemeiner entwickeln ließ und ich auch ein paar neue Erkenntnisse gewonnen habe, bietet sich diese synthetische Vorgehensweise an. Die Ergebnisse früherer Arbeiten sind dann meist Spezialfälle der hier dargestellten Ergebnisse.

# 2 Allgemeine Eigenschaften

## 2.1 Notation und Grundlagen

In diesem Abschnitt führe ich den Begriff der (k,v)-Matrix und die Eigenschaften $E_\lambda(u,w)$ ein. Diese ermöglichen oft eine einheitliche Behandlung von PA, induktiven PA und APA. Außerdem wird dadurch eine Verallgemeinerung von induktiven PA und APA nahegelegt, die ich s-PA genannt habe.

**(2.1) Definition** *Eine Matrix* $A = (a_{i,j})_{i\in I, j\in K}$ *mit Einträgen* $a_{i,j} \in V$*, deren Spalten mit einer Menge K indiziert sind, heißt* $(K,V)\text{-Matrix}$*. Diese heißt injektiv falls jede ihrer Zeilen eine injektive Abbildung ist. Kommt es nur auf die Elementanzahl der Mengen an, so spricht man von einer(k,V)-Matrix einer (K,v)-Matrix, bzw. einer (k,v)-Matrix, wobei k=|K| und v=|V|.*

*Sei A eine (K,V)-Matrix mit Bezeichnungen wie oben.*

- *Für* $i\in I$ *sei* $A(i) := (a_{i,j})_{j\in K}$ *die i-te Zeile von A.*
- *Für* $C\subseteq K$ *sei* $A_C := (a_{i,j})_{i\in I, j\in C}$ *die Einschränkung von A auf die Spaltenmenge C (*Restriktion*).*
- *Für* $C\subseteq K$*,* $W\subseteq V$ *sei* $A_C^W := (a_{i,j})_{i\in\{i\in I | A_C(i)\subseteq W\}, j\in C}$ *die Einschränkung von* $A_C$ *auf die Zeilen, die nur Elemente aus W enthalten.*
  *Setze* $A^W := A_K^W$ *(Residuum).*
- *Für* $C\subseteq K$*,* $W\subseteq V$ *sei* $A_C^{(W)} := (a_{i,j})_{i\in\{i\in I | A_C(i)\supseteq W\}, j\in C}$ *die Einschränkung von* $A_C$ *auf die Zeilen die W enthalten.*
  *Setze* $A^{(W)} := A_K^{(W)}$.
- *Die Anzahl der Zeilen von A sei mit* $\#A := |I|$ *bezeichnet.*

**Im folgenden seien alle (K,V)-Matrizen injektiv falls nicht ausdrücklich anders angegeben.**

**(2.2) Definition** *Eine (K,V)-Matrix A hat die Eigenschaft* $E_\lambda(u,w)$*, falls gilt:*

$$\forall_{\substack{W\subseteq V\\ |W|=w}} \; \forall_{\substack{U\subseteq W\\ |U|=u}} \; \forall_{\substack{C\subseteq K\\ |C|=w-u}} \; \#\left(A^{(W)}\right)_C^{(W-U)} = \lambda.$$

*Zur Gewöhnung in Worten: für alle* $U\subseteq W\subseteq V$ *mit* $|W|=w$ *und* $|U|=u$ *gilt: in den Zeilen, die die Einträge W enthalten, kommen, in jeder (w-u)-Menge von Spalten, die Einträge aus W-U genau* $\lambda$*-mal vor.*
*Will man nur ausdrücken, daß diese Anzahl eine Konstante ist, deren Wert aber nicht interessiert, so kann man "*$\lambda$*" weglassen. Will man die Parameter, zu denen* $\lambda$ *gehört, benennen, so schreibt man* $\lambda(u,w)$ *bzw.* $\lambda_A(u,w)$ *falls man auch die zugehörige Matrix benennen will.*

Da wir im folgenden häufiger Matrizen aneinanderfügen, ist es nützlich, dafür eine Notation einzuführen.

**(2.3) Definition** *Seien* $A = (a_{i,k})_{i\in I,k\in K}$ *und* $B = (b_{j,k})_{j\in J,k\in K}$ *Matrizen mit derselben Anzahl von Spalten, wähle die Indexmengen der Zeilen disjunkt und definiere:*

$$A \cup B := (c_{l,k})_{l\in I\cup J,k\in K} \text{ mit } c_{l,k} = \begin{cases} a_{l,k} & \text{für } l \in I \\ b_{l,k} & \text{für } l \in J \end{cases}$$

*Entsprechend sei* $\bigcup_i A_i$ *definiert.*

*Seien* $A = (a_{i,j})_{i\in I,j\in J}$ *und* $A' = (a_{i,j})_{i\in I',j\in J}$ *mit I'⊆I, eine Teilmatrix von A mit derselben Anzahl von Spalten, so definiere:*

$$A - A' := (a_{i,j})_{i\in I-I',j\in J}$$

**(2.4) Bemerkung** *Für u=0 reduziert sich die Definition einer (k,v)-Matrix mit Eigenschaft $E_\lambda(u,w)$ auf das folgende:*

> *Für alle W⊆V mit |W|=w, gilt:in A kommen die Einträge aus W in jeder w-Menge von Spalten genau λ-mal vor.*

**(2.5) Bemerkung** *Sei A eine (k,v)-Matrix mit Eigenschaft $E_\lambda(u,w)$. Es gilt:*

*a) Ist k>v, so ist A die leere Matrix (#A=0).*

*b) Ist w>k, w<1, u≥w oder u<w-k, so ist die Eigenschaft $E_\lambda(u,w)$ leer.*

*c) λ ist eine natürliche Zahl.*

*Beweis:*

a) Ist k>v, so ist die Bedingung der Injektivität verletzt und es gibt folglich keine solche Matrix.

b) Ist w>k, w<1, u>w oder u<w-k, so ist die Menge der Zeilen, über die eine Aussage gemacht wird, leer. Für u=w ist die Menge der Spalten, über die eine Aussage gemacht wird, leer.

c) λ ist als eine Anzahl definiert. ❑

**(2.6) Bemerkung** *Sei k=v und A eine (v,v)-Matrix mit Eigenschaft $E_\lambda(u,w)$ Es gilt:*

*a) $E_\lambda(u,w) \Leftrightarrow E_\lambda(0,w-u)$.*

*b) $E_\lambda(0,w) \Leftrightarrow E_\lambda(0,v-w)$.*

*Beweis*:

a) Ist k=v, so enthält jede Zeile von A aufgrund der Injektivität alle Elemente aus V. Somit gilt $\forall_{X\subseteq V} A^{(X)} = A$. Damit ist $\lambda = \#(A^{(W)})_C^{(W-U)} = \#A_C^{(W-U)}$ für alle U⊆W⊆V mit |W|=w, |U|=u und C⊆K mit |C|=w-u.Jedes W'⊆V mit |W'|=w-u läßt sich in der Form W-U darstellen, also folgt die Behauptung

b) Man verwende die Bijektion zwischen X⊆V und dem Komplement V-X⊆V ❑

Für den Beweis des folgenden Satzes benutze ich das

**Lemma von Kantor** [14]:

*Sei* $\mu_{A,B} := \begin{cases} 1 & \text{falls } B \subset A \\ 0 & \text{sonst} \end{cases}$, *wo A und B Teilmengen einer festen v-Menge V sind. Sei u,u'≤v. Betrachte die Inklusionsmatrix* $I(u,u') := (\mu_{A,B})_{A\in\wp^u(V),B\in\wp^{u'}(V)}$ *in Charakteristik 0. Dann gilt:*

*Die Inklusionsmatritzen I(u,u´) haben vollen Rang* $\mathrm{Min}\left(\binom{v}{u},\binom{v}{u'}\right)$.

**(2.7) Satz**

*a)* $E_\lambda(u,w) \Rightarrow E_\gamma(u-1,w-1)$ *mit* $\gamma = \lambda\frac{v-w-1}{k-w-1}$

*b) Ist w'<w und* $\binom{k}{w'-u} \le \binom{k}{w-u}$ *so gilt E(u,w)* $\Rightarrow$ *E(u,w') (vgl. Theorem 1.1 [15])*

*Beweis:*

a) Sei A eine (k,v)-Matrix mit Eigenschaft $E_\lambda(u,w)$. Seien U,W,U',W'⊆V, mit |W'|=w-1 und |U'|=u-1. Sei x∈V-(W') setze U=U'∪{x}, W=W'∪{x}. Sei C⊆K eine (w-u)-Menge von Spalten (beachte w-u = (w-1-(u-1)). Aus Eigenschaft E(u,w) folgt $\#\left(A^{(W)}\right)_C^{(W-U)} = \lambda$. Läßt man x durch V-W' laufen, so hat man die Zeilen, die W' enthalten, k-w+1 mal gezählt. Mit W'-U'=W-U und |V-W'|=v-w+1 erhält man

$$\#\left(A^{(W')}\right)_C^{(W'-U')} = \lambda(u,w)\frac{v-w+1}{k-w+1} = \lambda(u-1,w-1)$$

Insbesondere ist dies eine Konstante unabhängig von U,W und C.

b) Sei A eine (k,v)-Matrix mit Eigenschaft $E_\lambda(u,w)$. Sei U⊆W'⊆W⊆V, mit |W'|=w', |W|=w und |U|=u, sowie C,C'⊆K mit |C|=w-u und |C'|=w'-u. Die folgende Implikation ist zu zeigen:

$$\#\left(A^{(W)}\right)_C^{(W-U)} = \lambda \quad \Rightarrow \quad \#\left(A^{(W')}\right)_{C'}^{(W'-U)} = \text{const}$$

Man halte W' und U fest und definiere $I(C') := \#\left(A^{(W')}\right)_{C'}^{(W'-U)}$. Für jede (w-u)-Menge von Spalten C mit C'⊆C folgt aus E(u,w) und indem man W' zu einem passenden W ergänzt:

$$\sum_{C'\subseteq C} I(C') = \lambda\binom{k-(w'-u)}{w-w'}$$

Man erhält so ein System von $\binom{k}{w-u}$ Gleichungen in den $\binom{k}{w'-u}$ Unbekannten I(C'). Offensichtlich existiert die konstante Lösung

$$I(C') = \#\left(A^{(W')}\right)_{C'}^{(W'-U)} = \lambda\frac{\binom{k-(w'-u)}{w-w'}}{\binom{w-u}{w'-u}}$$

Dieser Ausdruck ist unabhängig von W',U.

Nach dem Lemma von Kantor hat das Gleichungssystem vollen Rang. Da nach Voraussetzung $\binom{k}{w'-u} \leq \binom{k}{w-u}$ d.h. die Zahl der Gleichungen mindestens so groß ist wie die Zahl der Unbekannten, ist die Lösung eindeutig. ❑

Es gibt die folgende Beziehung zwischen der Eigenschaft E(u,w) und t-Design's.

**(2.8) Satz** *Sei A eine (k,v)-Matrix, u>0. Dann sind äquivalent:*

*a) A hat die Eigenschaft $E_\lambda(u,w)$*

*b) Für jedes $E \subseteq V$, $|E|=(w-u)$ und jedes $S \subseteq K$, $|S|=(w-u)$ gilt: die Zeilen von A, die in den Spalten S die Einträge E stehen haben, bilden auf den Spalten K-S einen Design $u-(v-w+u,k-w+u,\lambda)$.*

*Beweis a⇒b:* Sei $E \subseteq V$, $S \subseteq K$ mit $|E|=|S|=(w-u)$. Man halte eine Menge S von Spalten und eine Menge E von Einträgen fest. Sei $U \subseteq V-E$ mit $|U|=u$. Aus E(u,w) folgt: es gibt $\lambda$ Zeilen, die die Einträge $U \cup E$, enthalten wobei die Einträge E in den Spalten S stehen. Folglich kommt in diesen Zeilen U in den Spalten K-S genau $\lambda$ mal vor. Also bilden diese Zeilen eingeschränkt auf die Spalten K-S ein $u-(v-w+u,k-w+u,\lambda)$.
Dieser Schluß ist offenbar umkehrbar. ❑

Zur späteren Benutzung notieren wir einige elementare Tatsachen:

**(2.9) Bemerkung**

*a) Existiert eine (k,v)-Matrix mit $E_\lambda(u,w)$, so gibt es für jedes $n \in \mathbb{N}$ eine (k,v)-Matrix mit $E_{n\lambda}(u,w)$.*

*b) Existiert eine (k,v)-Matrix mit $E_\lambda(0,w)$, so auch eine (k',v)-Matrix mit $E_\lambda(0,w)$ für jedes $k' \leq k$.*

*c) Die Anzahl #A der Zeilen einer (k,v)-Matrix A mit $E_\lambda(u,w)$ ist $\lambda \frac{\binom{v}{w}\binom{k}{w-u}}{\binom{k}{w}}$.*

*d) Bezeichne $S_n$ die symmetrische Gruppe des Grades n. Ist $\rho \in S_v, \sigma \in S_k$, $\tau \in S_{\#A}$ und $A=(a_{i,j})$ eine (k,v)-Matrix mit Eigenschaft $E_\lambda(u,w)$, so ist $(\rho,\sigma,\tau):(a_{i,j}) \mapsto (\rho a_{\sigma i,\tau j})$ ein Isomorphismus.*

*Beweis:*

a) Sei A eine (k,v)-Matrix mit $E_\lambda(u,w)$ so ist z.B. $\bigcup_{i=1}^{n} A$ eine (k,v)-Matrix mit $E_{n\lambda}(u,w)$.

b) Man streiche (k-k') Spalten aus der Matrix weg.

c) Man zähle die w-Mengen von Einträgen in den Zeilen von A. Man hat $\binom{v}{w}$ Möglichkeiten, eine solche w-Menge auszuwählen. Daraus wähle man eine feste (w-u)-Menge von Einträgen. Diese muß nach $E_\lambda(u,w)$ in jeder der $\binom{k}{w-u}$ Mengen der Kardinalität (w-u) von Spalten $\lambda$ mal in A vorkommen. Trivialerweise liefert eine

Zeile von A genau $\binom{k}{w}$ Mengen von w Einträge. Damit ist die Zahl der Zeilen gleich $\lambda\frac{\binom{v}{w}\binom{k}{w-u}}{\binom{k}{w}}$.

d) Offensichtlich sind die Injektivität und die Eigenschaft E(u,w) invariant unter den behaupteten Operationen, da die Aussagen über alle Teilmengen einer bestimmten Kardinalität von V gemacht werden. ❑

Nun zur Anwendung der neuen Begriffe auf PA. Zunächst definiere ich die s-PA, eine Verallgemeinerung der induktiven PA und der APA. Dies ermöglicht nicht nur eine einheitliche Behandlung der beiden Strukturen, sondern erweist sich sowohl in der Anwendung als auch in der Theorie als nützlich.

**(2.10) Definition** *Eine (k,v)-Matrix A, die die Eigenschaft E(u,w) für alle w≤t, 0≤u≤Min(w,s) erfüllt, heißt* $s\text{-}PA_\lambda(t,k,v)$ *wobei* $\lambda:=\lambda_A(0,t)$.

Es ergeben sich nun folgende Beziehungen:

**(2.11) Bemerkung**

*a) Eine (k,v)-Matrix mit $E_\lambda(0,t)$ ist ein $PA_\lambda(t,k,v)$.*

*b) Ein 0-$PA_\lambda(t,k,v)$ ist ein induktives $PA_\lambda(t,k,v)$.*

*c) Ein 1-$PA_\lambda(t,k,v)$ ist ein $APA_\lambda(t,k,v)$.*

*d) Ein s-$PA_\lambda(t,k,v)$ ist auch ein (s-j)-$PA(t-i,k,v)$ für alle $0\le i\le t$ und $0\le j\le s$.*

*e) Ein s-$PA_\lambda(t,k,v)$ ist für $s>t$ gleich einem t-$PA_\lambda(t,k,v)$, für $t>k$ gleich einem s-$PA_\lambda(k,k,v)$ und für $k>v$ nicht existent.*

*f) Ein (t-1)-$PA_\lambda(t,k,v)$ ist auch ein t-$PA_\lambda(t,k,v)$.*

*g) Ein $PA_\lambda(t,v,v)$ ist ein t-$PA_\lambda(t,v,v)$.*

*h) Existiert ein $PA_\lambda(t,v,v)$ so auch ein $PA_\lambda(v-t,v,v)$ (Theorem 1.4 [15]).*

*i) Existiert ein (0-)$PA_\lambda(t,k,v)$ so auch (0-)$PA_\lambda(t,k',v)$ für alle $k'\le k$ (Restriktion).*

*j) Ein $OD_\lambda(t,k,v)$ ist auch ein t-$PA_{\lambda t!}(t,k,v)$.*

*k) Ein 1-$PA_1(1,k,v)$, ein 2-$PA_2(2,2,v)$ und ein t-$PA_{(t!/2)}(t,t,v)$ $t\ge 3$ existieren für alle $v\ge k$.*

*Beweis*

a)..c) Nach Definition.

d) Man benutzt nur einen Teil der Eigenschaften die man hat.

e) Nach (2.5 b).

f) E(t,t) ist leer (2.5 b).

g) (2.6 a). h) (2.6 b). i) (2.9 b).

j) Ein $OD_\lambda(t,k,v)$ ist auch ein $OD_\gamma(w,k,v)$ für alle $w\le t$ (man lasse die nicht benötigten t-w Elemente durch alle v-w Teilmengen laufen). Für jedes $u\le w$ sei $U\subseteq W\subseteq V$ mit $|U|=u$ und $|W|=w$ sowie $C\subseteq K$ mit $|C|=w-u$. Es gilt: in jeder w-Menge von Spalten, die die Spalten C umfaßt, kommen die Einträge W in jeder möglichen Anordnung gleich

oft vor. Damit kommen insbesondere in den Zeilen, die W enthalten, die Einträge U in den Spalten C gleich oft vor. Also hat das $OD_\lambda(t,k,v)$ die Eigenschaft E(u,w) für alle $u \le w \le t$, es ist also ein t-PA (t,k,v).

k) Ein lateinisches Quadrat ist ein $PA_1(1,v,v)$, mit (2.9 b) erhält man ein $PA_1(1,k,v)$, die Bedingung E(1,1) ist leer. Man nehme alle 2-Teilmengen einer v-Menge; diese bilden ein (nicht induktives) $PA_1(2,2,v)$. Nun ersetze man jede Zeile durch ihre Bilder unter $S_2$ in der Operation auf den Spalten; dies liefert ein 2-$PA_2(2,2,v)$. Analog nehme man alle t-Teilmengen einer v-Menge und operiere mit der alternierenden Gruppe $A_t$ und erhalte einen t-$PA_{(t!/2)}(t,t,v)$. Daß die jeweiligen E(u,w) gelten, sieht man sofort. (Alternativ kann man (3.13) benutzen). ❑

Als Anwendung der Sätze über (k,v)-Matrizen mit Eigenschaft E(u,w) erhält man nun:

**(2.12) Folgerung**

*a) Es genügt in (2.10), die Eigenschaft E(u,w) zu fordern für w=t, $0 \le u \le s$ und für $t-s+1 \le w \le t$, u=s (siehe (2.7 a)).*

*b) Ist $(t-s) \le \lfloor k/2 \rfloor$, so genügt es in (2.10), die Eigenschaft E(u,w) zu fordern für w=t, $0 \le u \le s$ (siehe a) und (2.7 b)).*

**(2.13) Folgerung**

*a) Ist $t \le \lfloor k/2 \rfloor$, so ist jedes PA(t,k,v) induktiv (Theorem 1.1 [15] oder (2.11 b) und (2.7 b)).*

*b) Ist $t = \lfloor v/2 \rfloor$, so ist jedes PA(t,v,v) auch ein induktives PA(v,v,v) (siehe a) und (2.11 h)).*

**(2.14) Beispiel**

1.) Um zu sehen, daß die Matrix aus Beispiel (1.4) ein 2-$PA_3(3,3,4)$ ist, genügt es nach (2.12 b), E(0,3), E(1,3) und E(2,3) nachzuprüfen.

2.) Um zu sehen, daß die Matrix aus Beispiel (1.2) ein induktives PA(5,5,5) ist, genügt es nach (2.13 b) zu zeigen, daß sie ein PA(2,5,5) ist.

**(2.15) Folgerung** *Ist A ein s-$PA_\lambda(t,k,v)$, so gilt für alle $0 \le w \le t$ und $0 \le u \le Min(s,w)$:*

$$\lambda_A(u,w) = \lambda \frac{\binom{v}{t}\binom{k}{w}}{\binom{v}{w}\binom{k}{w-u}}$$

*Beweis:* Mit (2.9 c) und $\lambda=\lambda_A(0,t)$ gilt nach Definition $\lambda\binom{v}{t} = \#A = \lambda_A(u,w)\frac{\binom{v}{w}\binom{k}{w-u}}{\binom{k}{w}}$.

Daraus folgt die Behauptung. ❑

Sei A ein s-$PA_\lambda(t,k,v)$. Da $\lambda_A(u,w)$ stets eine natürliche Zahl ist, erhält man eine Teilbarkeitsbedingung an $\lambda$, und damit auch eine untere Schranke. Dies gibt Anlaß zu folgender

**(2.16) Definition**

$$\mu_s(t,k,v) := \mathrm{Min}\left\{\lambda \in \mathbb{N} \;\middle|\; \lambda \frac{\binom{v}{t}\binom{k}{w}}{\binom{v}{w}\binom{k}{w-u}} \in \mathbb{N}\ \left(\forall 0 \le w \le t \wedge 0 \le u \le \mathrm{Min}(w,s)\right)\right\}$$

*Ein s-PA$_\lambda$(t,k,v) heißt* optimal, *falls $\lambda = \mu_s(t,k,v)$. Wir nennen $\mu_s(t,k,v)$* das optimale $\lambda$. *Für s=0 ist $\mu_0(t,k,v)$ offensichtlich unabhängig von k und man schreibt $\mu_0(t,v)$.*

Damit erhält man unmittelbar aus (2.15) den folgenden:

**(2.17) Satz** *Für jedes s-PA$_\lambda$(t,k,v) gilt:*

$$\lambda \equiv 0 \ (\mathrm{mod}\ \mu_s(t,k,v))$$

**(2.18) Beispiel**

$$\mu_0(2,v) = \begin{cases} 1 & \text{für v ungerade} \\ 2 & \text{für v gerade} \end{cases} \qquad \mu_0(3,v) = \begin{cases} 1 & \text{für } v \equiv 2 (\mathrm{mod}\, 3) \\ 3 & \text{sonst} \end{cases}$$

$$\mu_1(2,k,v) = \begin{cases} 1 & \text{für k und v ungerade} \\ 2 & \text{sonst} \end{cases}$$

Man beachte, daß ein PA$_\lambda$(2,k,v) nach (2.13 a) für k≥3 stets induktiv ist. Dasselbe gilt für PA$_\lambda$(3,k,v), k≥5.

Es ist nicht bekannt, ob die (optimalen) 0-PA immer existieren. Dies sind die kleinsten offenen Probleme, was die Konstruktion optimaler 0-PA betrifft: PA$_2$(2,5,14), PA$_1$(2,6,15), PA$_2$(3,6,10) oder 0-PA$_2$(4,6,9). Mir ist kein Beispiel für die Nichtexistenz eines optimalen 0-PA bekannt, aber es existieren nicht immer optimale APA. So gibt es z.B. kein APA$_1$(2,3,5) (siehe z.B. [6]).

Eine ausführlichere Tabelle der $\mu_s$(t,k,v) und der offenen Probleme findet sich im Anhang.

## 2.2 Restriktion, Residuen und Aufblasen von PA

In diesem Abschnitt behandele ich rekursive Methoden zur Konstruktion von PA. Dazu gehört auch die (in-)direkte Produktkonstruktion (4.5), die allerdings nur für den Fall t=2 funktioniert und deshalb in Kapitel 4 behandelt wird. Die Restriktion ist für den Fall eines (0-)PA schon in (2.11 i) vorgekommen. Im allgemeinen liefert die folgende Bemerkung ein hinreichendes Kriterium.

**(2.19) Bemerkung** *Sei A eine (K,V)-Matrix mit Eigenschaft E$_\lambda$(u,w) und L⊆K. Ist für alle C⊆K mit |C|=w und C∩(K–L)≠∅ stets $A_C$ ist eine (C,V)-Matrix mit der Eigenschaft E(u,w), so ist die Restriktion $A_L$ von A auf L ist wieder eine (K,V)-Matrix mit Eigenschaft E$_\lambda$(u,w).*

*Beweis:* Seien U⊆W⊆V mit |U|=u und |W|=w. Sei D⊆L mit |D|=w-u. Durch Aufteilen der Zeilen, die W enthalten, in solche, bei denen W in den Spalten L liegt, und deren Komplement, erhält man:

$$\lambda_A(u,w) = \#\left(A^{(W)}\right)_D^{(W-U)} = \#\left(A_L{}^{(W)}\right)_D^{(W-U)} + \sum_{\{C \subseteq K \mid D \subseteq C \wedge C \cap (K-L) \neq \varnothing\}} \#\left(A_C{}^{(W)}\right)_D^{(W-U)}$$

Nach Voraussetzung haben alle im zweiten Summanden vorkommenden "$A_C$" die Eigenschaft E(u,w). Da natürlich $\#A_C$ für alle C dieselbe Zahl ist folgt mit (2.9 c), daß $\lambda_{A_C}(u,w)$ für alle Spaltenmengen C denselben Wert hat. Außerdem ist für $D \subseteq L$ auch $|\{C \subseteq K | D \subseteq C \wedge C \cap (K-L) \neq \emptyset\}|$ unabhängig von D. Also:

$$\lambda_A(u,w) = \#\left(A_L^{(W)}\right)_D^{(W-U)} + \sum_{\{C \subseteq K | D \subseteq C \wedge C \cap (K-L) \neq \emptyset\}} \lambda_{A_C}(u,w) = \#\left(A_L^{(W)}\right)_D^{(W-U)} + \text{const} \cdot \lambda_{A_C}(u,w)$$

Damit ist $\#\left(A_L^{(W)}\right)_D^{(W-U)}$ eine Konstante für alle $D \subseteq L$. Also hat $A_L$ die Eigenschaft E(u,w). ❑

**(2.20) Satz** *Sei $V' \subseteq V$ mit $|V'|=v-1$. Ist A eine (K,V)-Matrix mit Eigenschaft $E_\lambda(u,w)$, so ist das Residuum $A^{V'}$ (siehe (2.1)) eine (K,V')-Matrix mit Eigenschaft $E_\gamma(u-1,w-1)$ wobei* $\gamma = \lambda \frac{v-k}{k-w+1}$.

*Beweis:* Sei X:=V-V' also |X|=1, $U' \subseteq W' \subseteq V'$ mit |U'|=u-1 und |W'|=w-1. Da A eine (K,V)-Matrix mit Eigenschaft $E_\lambda(u,w)$ ist, gilt $\forall_{\substack{C \subseteq K \\ |C|=w-u}} \#\left(A^{(W' \cup X)}\right)_C^{(W-U)} = \lambda$. Da jede Zeile von $A^{(W' \cup X)}$ die Menge X enthält, liegt $A^{(W' \cup X)}$ in $A\text{-}A^{V'}$. Da W'-U'=W-U und da nach (2.7 a) A auch die Eigenschaft E(u-1,w-1) hat, gilt für alle $C \subseteq K$ mit |C|=w-u

$$\#\left((A^{V'})^{(W')}\right)_C^{(W'-U')} = \#\left(A^{(W')}\right)_C^{(W'-U')} - \#\left(A^{(W' \cup X)}\right)_C^{(W-U)} = \lambda_A(u-1,w-1) - \lambda_A(u,w)$$
$$\overset{(2.7\,a)}{=} \lambda \frac{v-w+1}{k-w+1} - \lambda = \lambda \frac{v-k}{k-w+1}$$

❑

**(2.21) Folgerung** *Sei $V' \subseteq V$, $|V'|=v-1$. Ist A ein s-$PA_\lambda(t,k,v)$, so ist das Residuum $A^{V'}$ ein (s-1)-$PA_\gamma(t-1,k,v-1)$ mit $\gamma=\lambda(v-k)/t$*

*Beweis* Ein s-$PA_\lambda(t,k,v)$ ist nach Definition eine (k,v)-Matrix mit Eigenschaft E(u,w) für alle $1 \le w \le t$, $0 \le u \le \text{Min}(w,s)$. Also ist $A^{V'}$ nach (2.20) eine (k,v-1)-Matrix mit Eigenschaft E(u-1,w-1) für alle $1 \le w \le t$, $0 \le u \le \text{Min}(w,s)$; diese ist nach Definition dann ein (s-1)-$PA_\gamma$(t-1,k,v-1) mit:

$$\gamma \overset{\text{def}}{=} \lambda_{(A^{V'})}(0,t-1) \overset{(2.20)}{=} \lambda_A(1,t) \frac{v-k}{k-t+1} \overset{(2.15)}{=} \lambda \frac{\binom{k}{t}}{\binom{k}{t-1}} \frac{v-k}{k-t+1} = \lambda \frac{v-k}{t}$$

❑

Die Tatsache, daß für alle $V' \subseteq V$ der Parameter $\lambda_{(A^{V'})}$ des Residuums natürlich auch die Teilbarkeitsbedingung (2.17) erfüllen muß, liefert keine schärfere Bedingung an $\lambda_A$ als (2.17). Dies hat Bierbrauer in [6] Theorem 5 gezeigt.

Als nächstes wird die PBD-Konstruktion behandelt; diese ist neben der schon erwähnten (in-)direkten Produktkonstruktion in den Arbeiten über PA das Haupthilfsmittel gewesen, um dort (A-)PA(t,k,v) zu konstruieren.

Für die Beweise der folgenden Sätze sind die nachstehenden Regeln für Binomialkoeffizienten nützlich, von deren Richtigkeit man sich unmittelbar überzeugen kann.

**(2.22)Bemerkung** *Es gelten:*

a) $$\frac{\binom{a-b}{c-d}}{\binom{a-c}{b-d}} = \frac{\binom{a}{c}\binom{c}{d}}{\binom{a}{b}\binom{b}{d}}$$

b) $$\sum_{i=0}^{c}\binom{a}{i}\binom{b}{c-i} = \binom{a+b}{c}$$

c) $$\binom{a}{b}+\binom{a}{b+1} = \binom{a+1}{b+1}$$

d) $$\binom{a-c}{b-c} = \frac{\binom{b}{c}\binom{a}{b}}{\binom{a}{c}}$$

**(2.23) Satz**

*a) Sei* $L \subseteq \mathbb{N}$ *und* $w \le t$. *Existiert ein t-*$(v,L,\mu)$ *und für alle* $l \in L$ *eine (k,l)-Matrix mit* $E_\lambda(u,w)$, *so existiert auch ein (k,v)-Matrix mit* $E_\gamma(u,w)$, *wobei*

$$\gamma = \lambda\mu\frac{\binom{v}{t}\binom{k}{w}}{\binom{v}{w}\binom{k}{w-u}}$$

*b) Sei* $L \subseteq \mathbb{N}$. *Existiert ein t-*$(v,L,\mu)$ *und für alle* $l \in L$ *ein s-*$PA_\lambda(t,k,l)$, *so existiert auch ein s-*$PA_{\lambda\mu}(t,k,v)$.

*Beweis:*

a) Seien $B_1 ... B_b$ die Blöcke eines t-$(v,L,\mu)$ und $A_i$ eine $(k,B_i)$Matrix mit $E_\lambda(u,w)$. Setze

$$A := \bigcup_{i=1}^{b} A_i$$

Seien $U \subseteq W \subseteq V$ mit $|W|=w$ und $|U|=u$, $C \subseteq K$ mit $|C|=w-u$ und $A_i$, $B_i$ wie oben. Nach Konstruktion gilt:

$$\lambda_{A_i}(u,w) = \lambda\frac{\binom{|B_i|}{t}\binom{k}{w}}{\binom{|B_i|}{w}\binom{k}{w-u}}, \text{ also ist}$$

$$\#(A^{(W)})_C^{(W-U)} = \sum_{\{B_i | W \subseteq B_i\}}\lambda_{A_i}(u,w) = \sum_{\{B_i | W \subseteq B_i\}}\lambda\frac{\binom{|B_i|}{t}\binom{k}{w}}{\binom{|B_i|}{w}\binom{k}{w-u}}$$

Durch doppelte Abzählung der Paare $(T,B_i)$ mit $|T|=t$, $W \subseteq T \subseteq B_i$ erhält man einerseits:

$$\#(T,B_i) = \mu\binom{v-w}{t-w} \overset{(2.22\ d)}{=} \mu\frac{\binom{v}{t}\binom{t}{w}}{\binom{v}{w}}$$

sowie andererseits:

$$\#(T,B_i)=\sum_{B_i|W\subseteq B_i}\binom{|B_i|-w}{t-w}\overset{(2.22\ d)}{=}\sum_{B_i|W\subseteq B_i}\frac{\binom{|B_i|}{t}}{\binom{|B_i|}{w}}\binom{t}{w}$$

Damit ergibt sich

$$\#(A^{(W)})_C^{(W-U)}=\lambda\mu\frac{\binom{v}{t}\binom{k}{w}}{\binom{v}{w}\binom{k}{w-u}}=\lambda_A(u,w),$$

also ist A eine (k,v)-Matrix mit $E_\gamma$(u,w) wie behauptet.

b) ist nun eine unmittelbare Folgerung. ❑

**(2.24) Beispiel**

1.) Wendet man den Satz (2.23) auf das 3-$PA_3$(3,3,3): $\begin{matrix}1&2&3\\2&3&1\\3&1&2\end{matrix}$ und den vollständigen Design 3-(4,3,4): $\begin{matrix}1&2&3\\1&2&4\\1&3&4\\2&3&4\end{matrix}$ an, so erhält man das $APA_3$(3,3,4) aus Beispiel (1.4). Insbesondere sieht man, daß es sogar ein 3-$PA_3$(3,3,4) ist.

2.) Nach (2.11 k) gibt es ein 4-$PA_{12}$(4,4,4), dies ist nach (2.11 d) auch ein 3-$PA_3$(3,4,4). Ich habe mit dem Computer ein 3-$PA_3$(3,4,6) gefunden (siehe Anhang C). Es gibt ein 3-(v,{4,6},1) für alle geraden v≥6 [11]. Damit erhalten wir nach (2.23) ein 3-$PA_3$(3,4,v) für alle geraden v≥6. Diese sind optimal als 3-PA, als 2-PA und als 1-PA und optimal als 0-PA für v≡0,1(mod 3) (siehe (2.16) oder Anhang A). Teirlink [30] hat $OD_1$(3,4,v) für alle 4≤v≠7 konstruiert. Diese sind nach (2.11 j) auch 3-$PA_6$(3,4,v). Da λ=6 optimal als 3-PA, als 2-PA und als 1-PA für t=3, k=4 und v ungerade erhalten wir: Es gibt optimale (3..1)-PA(3,4,v) für alle 4≤v≠7.

Ein interessanter Satz, der so ziemlich alle Tatsachen benutzt, die wir bis jetzt bewiesen haben ist:

**(2.25) Satz** (Bierbrauer Theorem 6 [6]) *Die Existenz eines optimales PA(⌊v/2⌋, v, v) impliziert die Existenz eines optimales t-PA(t, v, v+i) für i=0...⌊v/2⌋ und t=⌊v/2⌋+i....v.*

*Beweis:* Nach (2.13 b) und (2.11 g) ist das optimale PA(⌊v/2⌋,v,v) auch ein optimales t-$PA_\lambda$(t,v,v) für t=⌊v/2⌋..v. Verwendet man (2.23) mit dem vollständigen Design $t-(v+i,v,\binom{v+i-t}{i})$, so erhält man einen $t-PA_{\lambda\binom{v+i-t}{i}}(t,v,v+i)$, für i=0,...,⌊v/2⌋ und t=⌊v/2⌋+i...v. Durch i-fach wiederholte Residuenbildung (2.21) erhält man ein (t-i)-$PA_\gamma$(t-i, v, v), mit $\gamma=\lambda\frac{\binom{v+i-t}{i}}{\binom{t}{i}}$. Da t-i≥⌊v/2⌋ nach Wahl von t ist dieser PA wegen (2.13 b) und (2.11 g) äquivalent zu einem t-$PA_{\lambda'}$(t, v, v), mit:

$$\lambda'=\lambda\frac{\binom{v+i-t}{i}}{\binom{t}{i}}\frac{\binom{v}{t-i}}{\binom{v}{t}}=\frac{\binom{v-(t-i)}{t-(t-i)}}{\binom{t}{i}}\frac{\binom{v}{t-i}}{\binom{v}{t}}\overset{(2.22d)}{=}\lambda$$

Man sieht also, daß das erhaltene t-PA(t, v, v+i) das kleinstmögliche ist, denn sonst würde man als Residuum ein t-PA(t, v, v) erhalten, das kleiner als das optimale t-PA(t, v, v) wäre (was wegen (2.17) nicht möglich ist). Da Residuenbildung und die PBD-Konstruktion keine Verschärfung der Bedingung (2.17) liefern können (siehe Bierbrauer [6]), muß das t-PA(t, v, v+i) optimal sein. ❑

Wie wir im Laufe dieser Arbeit sehen werden kennen wir optimale PA($\lfloor v/2 \rfloor$ v, v) für $1 \le v \le 8$ und PA($\lfloor v/2 \rfloor$, v, v), die doppelt so groß als optimal sind, für t=9,10. Die durch den obigen Satz gelieferten t-PA(t, v, v+i) befinden sich im Anhang.

**(2.26) Satz** (Bierbrauer Theorem 7 [6]) *Sei* $s \ge \lfloor t/2 \rfloor$. *Es existiert ein s-PA*$_\lambda$*(t, t, v) genau dann wenn ein PA*$_\gamma$*(*$\lfloor t/2 \rfloor$*, t, t), mit* $\gamma = \frac{\lambda}{\binom{t}{\lfloor t/2 \rfloor}}$ *existiert.*

*Beweis:* Sei A ein s-PA$_\lambda$(t, t, v), T eine t-Menge von Einträgen von A. Die Eigenschaften E(0,t)...E(0,s) zeigen, daß $A^T$ ein 0-PA$_\gamma$(s, t, t) ist. Da $\#A^T=\lambda$ ist $\gamma = \frac{\lambda}{\binom{t}{s}}$. Insbesondere ist $A^T$ dann ein PA$_\gamma$($\lfloor t/2 \rfloor$, t, t), mit $\gamma = \frac{\lambda}{\binom{t}{\lfloor t/2 \rfloor}}$ .

Umgekehrt: Existiert ein PA$_\gamma$($\lfloor t/2 \rfloor$, t, t), mit $\gamma = \frac{\lambda}{\binom{t}{\lfloor t/2 \rfloor}}$ dieser ist nach (2.13 b) und (2.15) auch ein 0-PA$_\lambda$(t, t, t), so erhält man mit (2.23) unter Verwendung des vollständigen Design's t-(v,t,1), einen t-PA$_\lambda$(t, t, v). ❑

Sei A ein s-PA$_\lambda$(t,k,v). Um unter anderem die Beweise der folgenden beiden Sätze zu vereinfachen ist es nützlich, die Anzahlen $\lambda_A(u_+,u_-,w)$ und $\lambda_A(u_+,u_-,m_+w)$ einzuführen. Damit man bei den vielen "λ's" nicht durcheinanderkommt, erscheinen auch die schon bekannten im folgenden

**(2.27) Definition und Satz** *Sei* $A = (a_{i,j})_{i \in I, j \in K}$ *ein s-PA*$_\lambda$*(t,K,V), w≤t und 0≤u≤Min(s,w)*

*a)* $\lambda_A(w) := \#A_C^{(W)} = \lambda_A(0,w)$, *für alle* $W \subseteq V$ *mit* $|W|=w$ *und* $C \subseteq K$ *mit* $|C|=w$ *und es gilt* $\lambda_A(w) = \lambda \frac{\binom{v}{t}}{\binom{v}{w}}$

*b)* $\lambda_A(u,w) = \#\left(A^{(W)}\right)_C^{(W-U)} = \lambda_A(w) \frac{\binom{k}{w}}{\binom{k}{w-u}}$ *für alle* $U \subseteq W \subseteq V$ *mit* $|W|=w$ *und* $|U|=u$, *sowie* $C \subseteq K$ *mit* $|C|=w-u$

*c) Sei* $U_+ \subseteq U \subseteq W \subseteq V$, *mit* $|U_+|=u_+$, $|U|=u := u_- + u_+$ *und* $|W|=w$. *Ferner sei* $C \subseteq K$ *mit* $|C|=w-u$. *Setze* $U_- := U - U_+$

$$\lambda_A(u_+,u_-,w) := \left|\left\{ i \in I \,\middle|\, A(i) \supseteq W - U_-,\ A(i) \cap U_- = \varnothing,\ A_C(i) = W - U \right\}\right|$$

*In Worten: In den Zeilen, die die Einträge W-U- enthalten aber kein Element aus U-, kommen in den Spalten C die Einträge W-U genau* $\lambda_A(u_+,u_-,w)$ *mal vor.*

*Dies ist eine Konstante unabhängig von der Wahl von U-,U,W und C und es gilt:*

$$\lambda_A(u_+,u_-,w)=\lambda\frac{\binom{v}{t}\binom{v-w}{k+u_--w}}{\binom{v}{k}\binom{k}{w-u}}$$

*d) Sei $U_+\subseteq U\subseteq W\subseteq V$, mit $|U_+|=u_+$, $|U|=u:=u_-+u_+$ und $|W|=w$. Sei $0\le m_+\le w-u$ und $C\subseteq K$ mit $|C|=m_+$. Definiere:*

$$\lambda_A(u_+,u_-,m_+,w):=\left|\left\{i\in I\;\middle|\;\exists_{\substack{M_+\subseteq W-U\\|M_+|=m_+}}\left[A(i)\supseteq M_+\cup U_+,A(i)\cap\left(W-(M_+\cup U_+)\right)=\emptyset,A_C(i)=M_+\right]\right\}\right|$$

*In Worten: Betrachte die Zeilen, für die man eine $m_+$-Teilmenge $M_+$ von W-U so wählen kann, daß diese Zeile die Einträge $M_+\cup U_+$ enthält, aber kein Element von W-$(M_+\cup U_+)$. In diesen Zeilen kommt in den Spalten C genau $\lambda_A(u_+,u_-,m_+,w)$ mal eine $m_+$-Teilmenge von W-U vor.*

*Dies ist eine Konstante unabhängig von der Wahl von $U_+$,U,W und C und es gilt:*

$$\lambda_A(u_+,u_-,m_+,w)=\lambda\frac{\binom{v}{t}\binom{v-w}{k-u_+-m_+}}{\binom{v}{k}\binom{k}{m_+}}\binom{w-u}{m_+}$$

*Zusatz: Ist $k=t$ und $m_++u_+\le t$ so gelten die obigen Aussagen auch für $w\le v$ und $u_-\le w-m_+$.*

*e) Sei D ein t-(V,k,λ). Die Blockschnittzahl $\lambda_D(m,n)$, $m+n\le t$ ist definiert als die Zahl der Blöcke von D, die eine m-Menge $\subseteq V$ enthalten aber kein Element einer festgewählten dazu disjunkten n-Menge $\subseteq V$. Dann ist $\lambda_D(m,n)$ unabhängig von der Wahl dieser Mengen und es gilt:*

$$\lambda_D(m,n)=\lambda\frac{\binom{v}{t}\binom{v-m-n}{k-m}}{\binom{k}{t}\binom{v}{k}}$$

*Zusatz: Ist $k=t$ und $m\le t$ so gelten die obigen Aussagen auch für $m+n\le v$.*

*Nach Definition ist $\lambda=\lambda_A=\lambda_A(t)$, $\lambda_A(w)=\lambda_A(0,w)$, $\lambda_A(u,w)=\lambda_A(u,0,w)$, $\lambda_A(u_+,u_-,w)=\lambda_A(u_+,u_-,w-u_-,w)$.*
*Der Index A wird weggelassen, falls klar ist, auf welches PA sich λ bezieht.*

*Beweis:*

a),b) siehe (2.15)

c) Beweis durch Induktion nach $u_-$
Sei $u_-=0$. Es gilt:

$$\lambda(u,0,w):=\lambda(u,w)=\frac{\binom{v}{t}\binom{k}{w}}{\binom{v}{w}\binom{k}{w-u}}\overset{(2.22\ a)}{=}\frac{\binom{v}{t}\binom{v-w}{k-w}}{\binom{v}{k}\binom{k}{w-u}}$$

Damit ist der Induktionsanfang $u_-=0$ bewiesen.
Die Behauptung gelte für alle $v_-\le u_-$ und es sei $u<s$. Es gilt:

$$\lambda(u_+,u_-+1,w)=\lambda(u_+,u_-,w-1)-\lambda(u_++1,u_-,w)=\frac{\binom{v}{t}\binom{v-w+1}{k+u_--w+1}}{\binom{v}{k}\binom{k}{w-1-u}}-\frac{\binom{v}{t}\binom{v-w}{k+u_--w}}{\binom{v}{k}\binom{k}{w-1-u}}$$

$$\overset{(2.22\ c)}{=}\frac{\binom{v}{t}\binom{v-w}{k+u_--w+1}}{\binom{v}{k}\binom{k}{w-1-u}}=:\lambda(u_+,u_-+1,w).$$ Also ist c) bewiesen.

d) Sei $w\le t$. Beweis durch Induktion nach $m_-:=w-u-m_+$.
Der Induktionsanfang $m_-=0$ ($m_+=w-u$) ist c).
Die Behauptung gelte für alle $n_-\le m_-$ und sei $m_-<w-u$. Man zähle die gesuchten Zeilen wie folgt: für jedes $x\in W-U$ (davon gibt es w-u Stück) nehme man $\lambda_A(u_+,u_-,m_+w-1)$ Zeilen, die die Bedingungen für W-x statt W erfüllen. Darunter befinden sich für jede Spalte aus K-C (davon gibt es $k-m_+$ Stück) die $\lambda_A(u_+,u_-,m_++1w)$ Zeilen in denen ein Element aus W-U in dieser Spalte steht. Diese ziehe man ab (diese sind diejenigen, die die ursprüngliche Bedingung nicht erfüllen). Dann hat man jede der gesuchten Zeilen $|(W-U)-M_+|=(w-u-m_+)$ mal gezählt, also:

$$\lambda(u_+,u_-,m_+,w)=\frac{1}{w-u-m_+}\big((w-u)\lambda(u_+,u_-,m_+,w-1)-(k-m_+)\lambda(u_+,u_-,m_++1,w)\big)$$

$$=\frac{1}{w-u-m_+}\left((w-u)\lambda\frac{\binom{v}{t}\binom{v-w+1}{k-u_+-m_+}\binom{w-1-u}{m_+}}{\binom{v}{k}\binom{k}{m_+}}-(k-m_+)\lambda\frac{\binom{v}{t}\binom{v-w}{k-u_+-m_+-1}\binom{w-k}{m_++1}}{\binom{v}{k}\binom{k}{m_++1}}\right)$$

$$=\lambda\frac{\binom{v}{t}\binom{v-w}{k-u_+-m_+}\binom{w-k}{m_+}}{\binom{v}{k}\binom{k}{m_+}}\frac{1}{w-u-m_+}\cdot$$

$$\left((w-u)\frac{v-w+1}{v-w-k+u_++m_++1}\frac{w-u-m_+}{w-u}-(k-m_+)\frac{k-u_+-m_+}{v-w-k+u_++m_++1}\frac{w-k-m_+}{m_++1}\frac{m_++1}{k-m_+}\right)$$

$$=\lambda\frac{\binom{v}{t}\binom{v-w}{k-u_+-m_+}\binom{w-k}{m_+}}{\binom{v}{k}\binom{k}{m_+}}\left(\frac{v-w+1}{v-w-k+u_++m_++1}-\frac{k-u_+-m_+}{v-w-k+u_++m_++1}\right)=\frac{\binom{v}{t}\binom{v-w}{k-u_+-m_+}\binom{w-k}{m_+}}{\binom{v}{k}\binom{k}{m_+}}$$

$=:\lambda(u_+,u_-,m_+,w)$

Also gilt d) für $w\le t$.
Der Beweis des Zusatzes läßt sich durch direktes Abzählen führen. Sei k=t. Man hat $\binom{w-u}{m_+}$ Möglichkeiten, eine $m_+$-Menge $M_+$ in W-U zu wählen. Man hat $\binom{v-w}{t-m_+-u_+}$ Möglichkeiten eine $(t-m_+-u_+)$-Menge X in V-W zu wählen. In den Zeilen, die $X\cup U_+\cup M_+$ enthalten, kommt in den Spalten K-C die Menge $X\cup U$ genau $\lambda_A(t-m_+,t)$ mal vor. Also ist $\lambda_A(u_+,u_-,m_+w)=\binom{w-u}{m_+}\binom{v-w}{t-m_+-u_+}$ $\lambda_A(t-m_+,t)=\binom{w-u}{m_+}\binom{v-w}{t-m_+-u_+}\frac{\lambda}{\binom{t}{t-m_+}}$ wie behauptet.

e) Für $m+n\le t$ wohlbekannte Tatsache aus der Designtheorie siehe z.B. [34].
Zusatz: Sei w=t. Man erhält die Anzahl der gesuchten Blöcke indem man die Blöcke zählt, die eine feste m-Menge und eine beliebige (t-m)-Menge aus dem Komplement,

der gegebenen m-Menge vereinigt mit der gegebenen n-Menge, in V enthalten. Davon gibt es $\lambda\binom{v-m-n}{t-m}$ wie behauptet. ❑

**(2.28) Satz** *Existieren ein $s_1$-PA$_\lambda(t_1,k,v)$ und ein $s_2$-PA$_\mu(t_2,l,v-k)$, so auch ein $s$-PA$_\gamma(t,k+l,v)$ mit:*

$$\gamma = \lambda\mu\frac{\binom{v}{t_1}\binom{v-k}{t_2}}{\binom{v}{t}},$$

$$t = \begin{cases} \mathrm{Min}(t_1,t_2) & \text{falls } t_1 \neq k \wedge t_2 \neq l \\ t_1 & \text{falls } t_1 \neq k \wedge t_2 = l \\ t_2 & \text{falls } t_1 = k \wedge t_2 \neq l \\ t_1 + t_2 & \text{falls } t_1 = k \wedge t_2 = l \end{cases} \text{ und } s = \begin{cases} \mathrm{Min}(s_1,s_2) & \text{falls } s_1 \neq k \wedge s_2 \neq l \\ s_1 & \text{falls } s_1 \neq k \wedge s_2 = l \\ s_2 & \text{falls } s_1 = k \wedge s_2 \neq l \\ s_1 + s_2 & \text{falls } s_1 = k \wedge s_2 = l \end{cases}$$

*Beweis* Wähle die Indexmengen K und L disjunkt mit |K|=k und |L|=l. Sei $A = (a_{i,j})_{i\in I, j\in K}$ ein $s_1$-PA$_\lambda(t_1,K,V)$, $B(U) = (b(U)_{i,j})_{i\in I, j\in L}$ ein $s_2$-PA$_\mu(t_2,L,U)$ mit |U|=v-k. Die Matrix $C = (c_{p,j})_{p\in I\times J, j\in L\cup K}$ sei definiert durch

$$c_{(m,n),j} = \begin{cases} a_{m,j} & \text{für } j \in K \\ b(V - A(m))_{n,j} & \text{für } j \in L \end{cases}$$

und somit injektiv. C ist also die Matrix, die man erhält, wenn man, für jede Zeile z aus A hinter die #B Kopien von z die Zeilen der Matrix B schreibt. Dabei wählt man die Eintragsmenge von B als das Komplement der Einträge der Zeile z in V.
Sei w≤t, 0≤u≤Min(w,s) sowie U'⊆U⊆W⊆V mit |W|=w, |U|=u und |U'|=m. Sei D⊆K mit |D|=n und E⊆L mit |E|=w-u-n. Definiere:

$$x_m := \left|\left\{p \in I\times J \middle| C(p) \supseteq W, C_K(p) \subseteq U', C_{D\cup E}(p) = W - U\right\}\right|$$

Man kann aus den gegebenen $s_i$-PA nur solange Information über $x_m$ gewinnen solange gilt: |D|+|U'|= m+n≤$t_1$, |U'|=m≤$s_1$, w-m-n≤$t_2$ und u-m≤$s_2$. Die Summe $x(S) := \sum_{w-l-n\le m\le u} x_m$ ist dann gleich $\#\left(C^{(W)}\right)^{(W-U)}_{D\cup E}$ bei einer bestimmten Aufteilung (D,E) von W-U auf die Spalten. Also ist zu zeigen

$$x(S)= \lambda_C(u,w)= \lambda\mu\binom{v-k}{t_2}\frac{\binom{v}{t_1}\binom{k+l}{w}}{\binom{v}{w}\binom{k+l}{w-u}}$$

unabhängig von der gewählten Aufteilung (D,E).
Da A ein $s_1$-PA$_\lambda(t_1,k,v)$ ist, kommt eine n-Teilmenge von W-U in den Spalten D in den Zeilen, die U' enthalten aber kein Element aus dem Komplement, der gewählten n-Teilmenge vereinigt mit U', in W enthalten, $\lambda_A(m,u-m,n,w)$ mal vor. Man hat $\binom{u}{m}$ Möglichkeiten, U' in U zu wählen. Da B ein $s_2$-PA$_\mu(t_2,l,v-k)$ ist, werden die obigen Zeilen in C genau $\lambda_B(w-u-n,w-m-n)$ mal zu den Zeilen ergänzt, die in den Spalten D∪E die Einträge W-U stehen haben. Also gilt:

$$x_m = \binom{u}{m}\lambda_A(m,u-m,n,w)\lambda_B(w-u-n,w-m-n)$$

$$= \binom{u}{m}\lambda \frac{\binom{v}{t_1}\binom{w-u}{n}\binom{v-w}{k-m-n}}{\binom{v}{k}\binom{k}{n}}\mu \frac{\binom{v-k}{t_2}\binom{l}{w-m-n}}{\binom{v-k}{w-m-n}\binom{l}{w-u-n}}$$

$$= \lambda\mu\binom{v-k}{t_2}\binom{k+l}{w}\frac{\binom{v}{t_1}\binom{w-u}{n}}{\binom{v}{w}\binom{k}{n}\binom{l}{w-u-n}\binom{k+l}{w}}\binom{u}{m}\binom{l-w+k}{k-m-n}$$

Beachte die Identität :

$$\frac{\binom{v-w}{k-m-n}}{\binom{v-k}{w-m-n}} = \frac{\binom{v}{k}\binom{k}{m+n}}{\binom{v}{w}\binom{w}{m+n}} \quad \text{und} \quad \frac{\binom{l+k-k}{w-m-n}}{\binom{l+k-w}{k-m-n}} = \frac{\binom{k+l}{w}\binom{w}{m+n}}{\binom{k+l}{k}\binom{k}{m+n}} \qquad \text{(siehe (2.22 a))}$$

$$x(S) = \sum_{m=w-l-n}^{u} x_m = \lambda\mu\binom{v-k}{t_2}\binom{k+l}{w}\frac{\binom{v}{t_1}\binom{w-u}{n}}{\binom{v}{w}\binom{k}{n}\binom{l}{w-u-n}\binom{k+l}{w}}\sum_{m=w-l-n}^{u}\binom{u}{m}\binom{l-w+k}{k-m-n}$$

$$= \lambda\mu\binom{v-k}{t_2}\binom{k+l}{w}\frac{\binom{v}{t_1}\binom{w-u}{n}}{\binom{v}{w}\binom{k}{n}\binom{l}{w-u-n}\binom{k+l}{w}}\binom{l+k+u-w}{k-n} \qquad \text{(siehe (2.22 b))}$$

$$= \lambda\mu\binom{v-k}{t_2}\frac{\binom{v}{t_1}\binom{k+l}{w}}{\binom{v}{w}\binom{k+l}{w-u}} = \lambda_C(u,w) \quad \text{wo} \quad \frac{\binom{l+k+u-w}{k-n}}{\binom{l+k-k}{w-u-n}} = \frac{\binom{l+k}{k}\binom{k}{n}}{\binom{l+k}{w-u}\binom{w-u}{n}} \qquad \text{(siehe (2.22 a))}$$

❑

**(2.29) Beispiel**
Sei C ein 2-$PA_1$(2,2,3), D ein 2-(7,3,1) etwa:

C

| | |
|---|---|
| 1 | 2 |
| 2 | 3 |
| 3 | 1 |

D

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 1 | 4 | 7 |
| 1 | 5 | 6 |
| 2 | 4 | 6 |
| 2 | 5 | 7 |
| 3 | 4 | 5 |
| 3 | 6 | 7 |

Sei B das 0-$PA_{10}$(5,5,5) aus Beispiel (1.2) und A das 0-$PA_1$(2,2,7) das man nach (2.23) aus C und D erhält. Wir führen hier nun die Konstruktion der ersten Zeilen des 0-$PA_{210}$(7,7,7) (bzw.0-$PA_6$(3,7,7)), welches wir E nennen, gemäß (2.28) durch.

Die erste Zeile von A ist: "1 2". Die Eintragsmenge die man für B zur Ergänzung dieser Zeile benutzt: {3,4,5,6,7}. Damit ergeben sich die ersten 10 Zeilen von E wie folgt:

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 2 | 4 | 5 | 6 | 7 | 3 |
| 1 | 2 | 5 | 6 | 7 | 3 | 4 |
| 1 | 2 | 6 | 7 | 3 | 4 | 5 |
| 1 | 2 | 7 | 3 | 4 | 5 | 6 |
| 1 | 2 | 3 | 5 | 7 | 4 | 6 |
| 1 | 2 | 5 | 7 | 4 | 6 | 3 |
| 1 | 2 | 7 | 4 | 6 | 3 | 5 |
| 1 | 2 | 4 | 6 | 3 | 5 | 7 |
| 1 | 2 | 6 | 3 | 5 | 7 | 4 |

Die nächsten drei Zeile v von A sind: "2 3", "3 1" und "1 4". Die zugehörigen Eintragsmenge von B zur Ergänzung dieser Zeilen: {1,4,5,6,7}, {2,4,5,6,7} bzw. {2,3,5,6,7}. Damit ergeben sich die nächsten Drei mal 10 Zeilen von E wie folgt:

| | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 1 | 4 | 5 | 6 | 7 | | 3 | 1 | 2 | 4 | 5 | 6 | 7 | | 1 | 4 | 3 | 2 | 5 | 6 | 7 |
| 2 | 3 | 4 | 5 | 6 | 7 | 1 | | 3 | 1 | 4 | 5 | 6 | 7 | 2 | | 1 | 4 | 2 | 5 | 6 | 7 | 3 |
| 2 | 3 | 5 | 6 | 7 | 1 | 4 | | 3 | 1 | 5 | 6 | 7 | 2 | 4 | | 1 | 4 | 5 | 6 | 7 | 3 | 2 |
| 2 | 3 | 6 | 7 | 1 | 4 | 5 | | 3 | 1 | 6 | 7 | 2 | 4 | 5 | | 1 | 4 | 6 | 7 | 3 | 2 | 5 |
| 2 | 3 | 7 | 1 | 4 | 5 | 6 | | 3 | 1 | 7 | 2 | 4 | 5 | 6 | | 1 | 4 | 7 | 3 | 2 | 5 | 6 |
| 2 | 3 | 1 | 5 | 7 | 4 | 6 | | 3 | 1 | 2 | 5 | 7 | 4 | 6 | | 1 | 4 | 3 | 5 | 7 | 2 | 6 |
| 2 | 3 | 5 | 7 | 4 | 6 | 1 | | 3 | 1 | 5 | 7 | 4 | 6 | 2 | | 1 | 4 | 5 | 7 | 2 | 6 | 3 |
| 2 | 3 | 7 | 4 | 6 | 1 | 5 | | 3 | 1 | 7 | 4 | 6 | 2 | 5 | | 1 | 4 | 7 | 2 | 6 | 3 | 5 |
| 2 | 3 | 4 | 6 | 1 | 5 | 7 | | 3 | 1 | 4 | 6 | 2 | 5 | 7 | | 1 | 4 | 2 | 6 | 3 | 5 | 7 |
| 2 | 3 | 6 | 1 | 5 | 7 | 4 | | 3 | 1 | 6 | 2 | 5 | 7 | 4 | | 1 | 4 | 6 | 3 | 5 | 7 | 2 |

Führt man diese Konstruktion mit allen 21 Zeilen von A durch so erhält man die 210 Zeilen von E.
Übrigens ist E nur doppelt so groß wie ein optimales PA mit diesen Parametern. Meines Wissens ist außer dem von mir durch Computersuche gefundenen optimalen 0-$PA_3$(3,7,7) (siehe (3.26)) kein PA(3,7,7) in dieser Größenordnung bekannt.

**(2.30) Satz** *Existieren ein $s_1$-$PA_\lambda(t_1,r,k)$, ein $t_1$-$(v,k,\mu)$ und ein $s_2$-$PA_\nu(t_2,l,v-k)$, so auch ein s-$PA_\gamma(t,r+l,v)$ mit:*

$$\gamma = \lambda\mu\nu\frac{\binom{v}{t_1}\binom{v-k}{t_2}}{\binom{v}{t}},$$

$$t = \begin{cases} \mathrm{Min}(t_1,t_2) & \textit{falls } t_1 \neq k \wedge t_2 \neq l \\ t_1 & \textit{falls } t_1 \neq k \wedge t_2 = l \\ t_2 & \textit{falls } t_1 = k \wedge t_2 \neq l \\ t_1 + t_2 & \textit{falls } t_1 = k \wedge t_2 = l \end{cases} \textit{ und } s = \begin{cases} \mathrm{Min}(s_1,s_2) & \textit{falls } s_1 \neq k \wedge s_2 \neq l \\ s_1 & \textit{falls } s_1 \neq k \wedge s_2 = l \\ s_2 & \textit{falls } s_1 = k \wedge s_2 \neq l \\ s_1 + s_2 & \textit{falls } s_1 = k \wedge s_2 = l \end{cases}.$$

*Beweis* Ähnlich zu dem vorherigen, nur daß die Abzählung einfacher ist, insbesondere benötigt man nicht (2.27 d).
Wähle die Indexmengen R und L disjunkt mit |R|=r und |L|=l. Sei F ein $t_1$-$(v,k,\mu)$ und $B_i$, $i \in I$ dessen Blöcke. Sei $A_i$ ein $s_1$-$PA_\lambda(t_1,R,B_i)$, $A_i = (a^i_{j,m})_{j\in J, m\in R}$, sowie B(H) ein $s_2$-$PA_\nu(t_2,L,H)$ mit |H|=v-k, $B(H) = (b(H)_{k,n})_{k\in K, n\in L}$. Die Matrix $C = (c_{p,j})_{p\in I\times J\times K, j\in L\cup R}$ sei definiert durch

$$c_{(i,m,n),j} = \begin{cases} a^i_{m,j} & \text{für } j \in R \\ b(V - B_i)_{n,j} & \text{für } j \in L \end{cases}$$

und somit injektiv. Sei $w \le t$, $0 \le u \le \mathrm{Min}(w,s)$, $U \subseteq W \subseteq V$, $U' \subseteq W' \subseteq V$ mit |W|=w und |U|=u, $U' \subseteq U$, $W' \subseteq W$ mit |U'|=m und |W'|=m+n. Sei $D \subseteq K$, |D|=n, $E \subseteq L$, |E|=w-u-n, definiere:

$$x_m := \left|\left\{p \in I\times J\times K \,\middle|\, C(p) \supseteq W, C_L(p) \subseteq V - W', C_D(p) = W' - U', C_E(p) = (W - W') - (U - U')\right\}\right|$$

Man kann aus den gegebenen $s_i$-PA nur solange Information über $x_m$ gewinnen solange gilt: $|W'|=m+n \le t_1$, $|U'|=m \le s_1$, $w-m-n \le t_2$ und $u-m \le s_2$ . Wie im vorherigen Beweis ist also zu zeigen:

$$x(S)= \lambda_C(u,w)= \lambda\mu\nu\binom{v-k}{t_2}\frac{\binom{v}{t_1}\binom{u+l}{w}}{\binom{v}{w}\binom{u+l}{w-u}}$$

unabhängig von der gewählten Aufteilung (D,E).
In den Zeilen zu den Blöcken, die W' enthalten, aber kein Element aus W-W' enthalten (deren Anzahl ist die Blockschnittzahl $\lambda_F(|W'|,|W-W'|)$, siehe (2.27 e)), hat man $\binom{w-u}{n}$ Möglichkeiten, W'-U' in W-U zu wählen. Da $A_i$ ein $s_1$-$PA_\lambda(t_1,r,k)$ ist, kommt W'-U' in den Spalten D der Zeilen, die W' enthalten, $\lambda_A(m,m+n)$ mal vor. Man hat $\binom{u}{m}$ Möglichkeiten, U' in U zu wählen. Da B ein $s_2$-$PA_\mu(t_2,l,v-k)$ ist, werden die obigen Zeilen in C genau $\lambda_B(w-u-m,w-m-n)$ mal so ergänzt, daß die Teilmengen (W-W')-(U-U') von W-U in den Spalten E stehen. Also gilt:

$$x_m = \binom{u}{m}\binom{w-u}{n}\lambda_F(m+n,w-m-n)\lambda_A(m,m+n)\lambda_B(w-u-m,w-m-n)$$

$$= \binom{u}{m}\binom{w-u}{n}\mu\frac{\binom{v}{t_1}\binom{v-w}{k-m-n}}{\binom{k}{t_1}\binom{v}{k}}\lambda\frac{\binom{k}{t_1}\binom{r}{m+n}}{\binom{k}{m+n}\binom{r}{n}}\nu\frac{\binom{v-k}{t_2}\binom{l}{w-m-n}}{\binom{v-k}{w-m-n}\binom{l}{w-u-n}}$$

$$= \lambda\mu\nu\binom{v-k}{t_2}\binom{l+r}{w}\frac{\binom{v}{t_1}\binom{w-u}{n}}{\binom{v}{w}\binom{r}{n}\binom{l}{w-u-n}\binom{l+r}{r}}\binom{u}{m}\binom{l+r-w}{r-m-n}$$

Beachte die Identität :

$$\frac{\binom{v-w}{k-m-n}}{\binom{v-k}{w-m-n}} = \frac{\binom{v}{k}\binom{k}{m+n}}{\binom{v}{w}\binom{w}{m+n}} \text{ und } \frac{\binom{l+r-r}{w-m-n}}{\binom{l+r-w}{r-m-n}} = \frac{\binom{l+r}{w}\binom{w}{m+n}}{\binom{l+r}{r}\binom{r}{m+n}} \text{ siehe (2.22a)}$$

$$x(S) = \sum_{m=w-l+n}^{u} x_m = \lambda\mu\nu\binom{v-k}{t_2}\binom{l+r}{w}\frac{\binom{v}{t_1}\binom{w-u}{n}}{\binom{v}{w}\binom{r}{n}\binom{l}{w-u-n}\binom{l+r}{r}}\sum_{m=w-l+n}^{u}\binom{u}{m}\binom{l+r-w}{r-m-n}$$

$$= \lambda\mu\nu\binom{v-k}{t_2}\binom{l+r}{w}\frac{\binom{v}{t_1}\binom{w-u}{n}}{\binom{v}{w}\binom{r}{n}\binom{l}{w-u-n}\binom{l+r}{r}}\binom{l+r+u-w}{r-n} \quad \text{siehe (2.22 b)}$$

$$= \lambda\mu\nu\binom{v-k}{t_2}\frac{\binom{v}{t_1}\binom{l+r}{w}}{\binom{v}{w}\binom{l+r}{w-u}} = \lambda_C(u,w) \quad \text{wo } \frac{\binom{l+r+u-w}{r+n}}{\binom{l+r-r}{w-u-n}} = \frac{\binom{l+r}{r}\binom{r}{n}}{\binom{l+r}{w-u}\binom{w-u}{n}} \text{ siehe (2.22 a)}$$

❑

**(2.31) Beispiel** Um einen Vergleich zu haben, nehmen wir als Ausgangsstrukturen das 2-$PA_1$(2,2,3): C und das 2-(7,3,1):D aus Beispiel (2.29) sowie das 3-$PA_3$(3,3,4) aus Beispiel (1.4) dieses nennen wir B, auch wenn das 2-$PA_{12}$(2,5,7) E das wir daraus nach (2.30) erhalten werden nicht sonderlich interessant ist. Sei A wieder das 0-$PA_1$(2,2,7) das man nach (2.21) aus C und D erhält. Man erhält die ersten 12 Zeilen von E indem man die erste Zeile von A, "1 2", durch die Zeilen von B ergänzt. Hier ist die Eintragsmenge von B das Komplement des Blockes, mit dem die erste Zeile von A erzeugt wurde, also:{4,5,6,7}. damit sehen die ersten 12 Zeilen von E folgendermaßen aus.

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 4 | 5 | 6 |
| 1 | 2 | 5 | 6 | 4 |
| 1 | 2 | 6 | 4 | 5 |
| 1 | 2 | 4 | 5 | 7 |
| 1 | 2 | 5 | 7 | 4 |
| 1 | 2 | 7 | 4 | 5 |
| 1 | 2 | 4 | 6 | 7 |
| 1 | 2 | 6 | 7 | 4 |
| 1 | 2 | 7 | 4 | 6 |
| 1 | 2 | 5 | 6 | 7 |
| 1 | 2 | 6 | 7 | 5 |
| 1 | 2 | 7 | 5 | 6 |

Da die nächsten beiden Zeilen von A, "1 3" und"3 2", mit demselben Block von D konstruiert worden sind, werden sie mit demselben B ergänzt. Erst die nächste Zeile von A, "1 4" wird die Eintragsmenge von B geändert, nämlich :{3,5,6,7}. Damit ergeben sich die nächsten 36 Zeilen von E als:

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 3 | 1 | 4 | 5 | 6 | 1 | 4 | 3 | 5 | 6 |
| 2 | 3 | 5 | 6 | 4 | 3 | 1 | 5 | 6 | 4 | 1 | 4 | 5 | 6 | 3 |
| 2 | 3 | 6 | 4 | 5 | 3 | 1 | 6 | 4 | 5 | 1 | 4 | 6 | 3 | 5 |
| 2 | 3 | 4 | 5 | 7 | 3 | 1 | 4 | 5 | 7 | 1 | 4 | 3 | 5 | 7 |
| 2 | 3 | 5 | 7 | 4 | 3 | 1 | 5 | 7 | 4 | 1 | 4 | 5 | 7 | 3 |
| 2 | 3 | 7 | 4 | 5 | 3 | 1 | 7 | 4 | 5 | 1 | 4 | 7 | 3 | 5 |
| 2 | 3 | 4 | 6 | 7 | 3 | 1 | 4 | 6 | 7 | 1 | 4 | 3 | 6 | 7 |
| 2 | 3 | 6 | 7 | 4 | 3 | 1 | 6 | 7 | 4 | 1 | 4 | 6 | 7 | 3 |
| 2 | 3 | 7 | 4 | 6 | 3 | 1 | 7 | 4 | 6 | 1 | 4 | 7 | 3 | 6 |
| 2 | 3 | 5 | 6 | 7 | 3 | 1 | 5 | 6 | 7 | 1 | 4 | 5 | 6 | 7 |
| 2 | 3 | 6 | 7 | 5 | 3 | 1 | 6 | 7 | 5 | 1 | 4 | 6 | 7 | 5 |
| 2 | 3 | 7 | 5 | 6 | 3 | 1 | 7 | 5 | 6 | 1 | 4 | 7 | 5 | 6 |

Führt man diese Konstruktion mit allen 21 Zeilen von A durch so erhält man die 252 Zeilen von E.

Durch Kombination von (2.23 b) und (2.28) lassen sich s-PA konstruieren, deren Parameter dieselben sind wie in (2.30) mit Ausnahme des Wertes von $\lambda$. Der Vollständigkeit halber ist auch (2.30) explizit erwähnt:

**(2.32) Folgerungen** *Existieren ein $s_1$-PA$_\lambda(t_1,r,k)$ und ein $t_1$-$(v,k,\mu)$, so gilt*

*a) existiert außerdem ein $s_2$-PA$_\nu(t_2,l,v-k)$, so auch ein s-PA$_\gamma(t,r+l,v)$ mit*
$$\gamma = \lambda\mu\nu\binom{v-k}{t_2}\frac{\binom{v}{t_1}}{\binom{v}{t}}$$

*b) existiert außerdem ein $s_2$-PA$_\nu(t_2,l,k-r)$, so auch ein s-PA$_\gamma(t,r+l,v)$ mit*
$$\gamma = \lambda\mu\nu\binom{k-r}{t_2}\frac{\binom{v}{t_1}}{\binom{v}{t}}$$

*c) existiert außerdem ein $s_2$-PA$_\nu(t_2,l,v-r)$, so auch ein s-PA$_\gamma(t,r+l,v)$ mit*
$$\gamma = \lambda\mu\nu\binom{v-r}{t_2}\frac{\binom{v}{t_1}}{\binom{v}{t}}$$

*d) existiert außerdem ein $s_2$-PA$_\nu(t_2,l,v-r)$, das ein $s_2$-PA$_{\nu'}(t_2,l,v-k)$ enthält, so auch ein s-PA$_\gamma(t,r+l,v)$ mit* $\gamma = \lambda\mu\left[\nu\binom{v-r}{t_2} - \nu'\binom{v-k}{t_2}\right]\frac{\binom{v}{t_1}}{\binom{v}{t}}$

*Wobei s,t wie in (2.30)*

*Beweis:* a) (2.30).

b) Man wende erst (2.28) und dann (2.23 b) an.

c) Man wende erst (2.23 b) und dann (2.28) an.

d) Man verfahre wie in c), wobei man im (2.28) dafür sorgt, daß die Eintragsmenge des $s_2$-$PA_v(t_2,l,v-k)$ gerade das Komplement des Blockes ist mit dem dieser Abschnitt in (2.23 b) konstruiert wird. Man erhält so das s-PA aus a) als Teilmatrix. Deren Komplement in der Gesamtmatrix ist das gesuchte s-PA. ❑

**(2.33) Folgerungen** *Es existiere ein s-*$PA_\lambda(t,l,k)$*. Dann gilt:*

*a) Existiert außerdem ein t-*$(v,k,\mu)$*, so existiert ein s-*$PA_{\lambda\mu(v-k)}(t,l+1,v)$*, falls* $l<v$*.*

*b) Existiert außerdem ein t-*$(v,k,\mu)$*, so existiert ein s-*$PA_{\lambda\mu(k-l)}(t,l+1,v)$*, falls* $l<k$*.*

*c) Es existiert ein s-*$PA_{\lambda(k+1-t)}(t,l+1,k+1)$*.*

*d) Es existiert ein* $s-PA_{x\lambda}\binom{k-l}{x}(t,l+x,k)$ *x=1,2,3, falls* $l+x\leq k$*. Insbesondere läßt sich ein s-*$PA_\lambda(t,v-1,v)$ *immer (eindeutig) zu einem s-*$PA_\lambda(t,v,v)$ *ergänzen*

*Beweis:*

a) Trivialerweise existiert ein 1-$PA_1(1,1,v)$ für alle v. Behauptung folgt mit (2.30).

b) Es existiert ein 1-$PA_1(1,1,v)$ für alle v. Behauptung folgt mit (2.32 b).

c) Man nehme in a) den vollständigen Design t-(v+1,v,v+1-t)

d) Man nehme die x-$PA_x(x,x,v)$ x=1,2,3 aus (2.11 k). Die Behauptung folgt mit (2.28)

**(2.34) Bemerkung**

*a) (2.33 a) ist im Spezialfall s=1 und l=k Theorem 2.8 [32]*

*b) (2.33 c) ist im Spezialfall s=1 und l=k Theorem 2.2 [32]*

**(2.35) Beispiel** Es existiert ein 4-$PA_2(4,5,5)$ (siehe Beispiel (1.2)) und ein 4-(11,5,1) (siehe [1]) damit nach (2.33 a) ein 4-$PA_{12}(4,6,11)$. Dieser ist schon optimal als 1-PA.(Optimalität siehe (2.17) und Anhang A).

**(2.36) Beispiel** Es existiert ein $PA_1(2,7,7)$ und ein 2-(21,7,3) (siehe [1]). Damit existiert nach (2.23 b) ein $PA_3(2,7,21)$. Mit dem 2-(85,21,5) (siehe [1]) existiert nach (2.33 b) ein 2-$PA_{210}(2,7,85)$. Dieser ist kleiner als der 2-PA(2,7,85) den man erhält wenn man (2.33 a) auf das $PA_1(2,7,21)$ und den 2-(85,21,5) anwendet.

**(2.37) Beispiel** Auch mit (2.33 c) lassen sich neue optimale PA erzeugen. Die nachfolgenden Beispiele, haben bis auf das erste nur den Schönheitsfehler, daß die Ausgangs-PA noch nicht bekannt sind. Das $PA_3(3,6,6)$ wurde auch schon in [15] auf andere Weise gefunden.

Die Existenz eines $PA_1(3,5,5)$ impliziert die eines $PA_3(3,6,6)$ (optimal)

Die Existenz eines $PA_2(5,9,9)$ impliziert die eines $PA_{10}(5,10,10)$ (optimal)

Die Existenz eines $PA_1(4,15,15)$ impliziert die eines $PA_{12}(4,16,16)$ (optimal)

Die Existenz eines $PA_3(6,15,15)$ impliziert die eines $PA_{30}(6,16,16)$ (optimal)

## 2.3 Verwendung von (k,v)-Matrizen in der Kryptographie

**Modell des Kryptosystems:**

Sei $A = (a_{i,j})_{i\in I, j\in K}$ eine (K,V)-Matrix. Sei K die Menge der Quellenzustände (das sind die unverschlüsselten Nachrichten). Jeder Quellenzustand $k\in K$ soll unabhängig mit fester vorgegebener Wahrscheinlichkeit P(k) gesendet werden. Die Zeilen $f_i:=A(i)$ sind die Schlüssel. Diese werden mit gleicher Wahrscheinlichkeit $P(k):=1/b$ mit $b:=|I|$, verwendet. Das Kryptogramm (die verschlüsselte Nachricht) ist der Eintrag $f_i(k):=a_{i,k}\in V$.

Zur Vereinfachung der Untersuchung nehmen wir an, daß die Quellenzustände, die mit demselben Schlüssel kodiert werden, alle verschieden sind. Desweiteren nehmen wir an, daß die Reihenfolge der Quellenzustände, also auch die der Kryptogramme, die mit demselben Schlüssel kodiert werden, unerheblich ist.

Stinson [27] sagt, daß diese Einschränkungen nicht strikt nötig sind.

**Idee der perfekten t-fachen Geheimhaltung:**

Bei bis zu t-maliger Verwendung des gleichen Schlüssels erhält der Gegner durch Kenntnis der zugehörigen Kryptogramme keine Information über die zugrundeliegenden Quellenzustände. Dies ist beweisbar, also insbesondere unabhängig von der verfügbaren Rechnerkapazität und eventuellen Fortschritten in der Konstruktion von Algorithmen. Konkret übersetzt sich die obige Aussage in eine Gleichheit von Wahrscheinlichkeiten: Sei dem Gegner eine Menge T von w Kryptogrammen bekannt, die unter Verwendung desselben Schlüssels entstanden (damit $0\le w\le t$). Sei E eine Menge von w Quellenzuständen. Wir wollen die folgenden zwei Wahrscheinlichkeiten miteinander vergleichen:

1. Die Wahrscheinlichkeit P(E), daß w aufeinanderfolgende Quellenzustände die Menge E bilden.
2. Die bedingte Wahrscheinlichkeit P(E|T). Dies ist die Verteilung auf der Quelle, wie sie der Gegner aufgrund seiner Kenntnis der Menge T von Kryptogrammen berechnen kann.

Wir sagen, daß die Matrix A perfekte t-fache Geheimhaltung liefert, falls für alle $E\subseteq K$ mit $|E|=w$ und $T\subseteq V$ mit $|T|=w$ und $0\le w\le t$ gilt:

$$P(E|T)=P(E).$$

Also hätte der Gegner genausogut raten können.

**(2.38) Satz** *Ein 0-$PA_\lambda(t,k,v)$ verschafft perfekte t-fache Geheimhaltung*

*Beweis:* Sei $E\subseteq K$ mit $|E|=w$ und $T\subseteq V$ mit $|T|=w$. Für alle $0\le w\le t$ gilt:

$$P(E|T) = \frac{P(T\mid E)P(E)}{P(T)} = \frac{\lambda_A(w)(1/b)P(E)}{\sum_{\{f|T\subseteq f(K)\}} P(f)P(f^{-1}(T))}$$

$$= \frac{\lambda(w)(1/b)P(E)}{1/b \sum_{\{D\subseteq K|w=|D|\}} \sum_{\left\{f\middle|D=f^{-1}(T)\right\}} P(D)} = \frac{\lambda(w)(1/b)P(E)}{(1/b)\lambda(w) \sum_{\{D\subseteq K|w=|D|\}} P(D)} = P(E)$$

❑

Ein Code, der t-fache Geheimhaltung erzielt, hat, wie man sofort sieht, mindestens $\binom{k}{t}$ Schlüssel. Ein $PA_1(t,k,k)$ ist also ein Code mit minimaler Schlüsselanzahl. Da es wünschenswert ist, die Zahl der Schlüssel möglichst klein zu halten, sind hier PA mit möglichst kleinem $\lambda$ gesucht.

**Idee der Authentikation:**

Das Ziel des Gegners ist es, Kryptogramme einzuschmuggeln, die der Empfänger für authentisch hält. Man hat Sicherheit gegen Spoofing der Ordnung (w-u) der Stärke u (frei nach Stinson), wenn die Wahrscheinlichkeit, daß, wenn der Gegner w-u Kryptogramme kennt und dazu u eigene sendet, diese Kryptogramme als authentisch angenommen werden, genauso groß ist, als hätte er dies ohne die Kenntnis der w-u Kryptogramme getan.

In Formeln: Seien $T_0,T_1 \subseteq V$ $|T_0|=w-u, |T_1|=u$ . Wir fordern:

$$P(T_0 \cup T_1 | T_0) = \frac{\binom{k-w+u}{u}}{\binom{v-w+u}{u}}$$

Man beachte, daß Authentikation nur im Fall v>k möglich ist.

**(2.39) Satz** *Eine (K,V)-Matrix mit E(u,w) verschafft Sicherheit gegen Spoofing der Ordnung (w-u) und der Stärke u*

*Beweis:*

$$p := P(T_0 \cup T_1 | T_0) = \frac{\sum_{\{f \in A | f(K) \supseteq T_0 \cup T_1\}} P(f)P(f^{-1}(T_0))}{\sum_{\{f \in A | f(K) \supseteq T_0\}} P(f)P(f^{-1}(T_0))}.$$

Nach Voraussetzung ist P(f)=1/b. Die Eigenschaft E(u,w) impliziert E(0,w-u) (siehe (2.7 a)). Da E(0,w-u) gilt, läßt sich der Nenner schreiben als:

$$\sum_{\{f \in A | f(K) \supseteq T_0\}} P(f)P(f^{-1}(T_0)) = \frac{1}{b}\lambda(0, w-u) \sum_{\{D \subseteq K || D|=w-u\}} P(D) = \frac{1}{b}\lambda(0, w-u)$$

Aus E(u,w) ergibt sich folgende Umformung für den Zähler:

$$\sum_{\{f \in A | f(K) \supseteq T_0 \cup T_1\}} P(f)P(f^{-1}(T_0)) = \frac{1}{b} \sum_{\{D \subseteq K || D|=w-u\}} P(D) \left| \{ f | f(D) = E_0, f(K) \supseteq E_1 \} \right|$$

$$= \frac{1}{b} \sum_{\{D \subseteq K || D|=w-u\}} P(D)\lambda(u,w) = \frac{1}{b}\lambda(u,w) ,$$

$$\text{also } p = \frac{\lambda(u,w)}{\lambda(0,w-u)} = \frac{\binom{v}{w-u}\binom{k}{w}}{\binom{v}{w}\binom{k}{w-u}} \overset{(2.22\ a)}{=} \frac{\binom{k-w+u}{u}}{\binom{v-w+u}{u}}$$

❑

**(2.40) Folgerung** *Ein s-$PA_\lambda(t,k,v)$ liefert t-fache Geheimhaltung und Schutz gegen Spoofing der Ordnung (w-u) und der Stärke u für alle $0 \leq u \leq Min(s,w)$, $0 \leq w \leq t$.*

Für s=1 wird dies in [25],[26]und[27] behandelt.

# 3 PA und Gruppen

## 3.1 PA als Teilmengen von Gruppen

Nun wird es Zeit, PA auch explizit zu konstruieren, damit man die bisher erarbeitete Theorie auch zur Anwendung bringen kann. Als erstes werden wir sehen, daß t-homogene Gruppen PA(t,v,v) liefern. Da wir an PA mit möglichst kleinem $\lambda$ interessiert sind, brauchen wir auch möglichst kleine t-homogene Gruppen. Als Konsequenz der Klassifikation der endlichen einfachen Gruppen, sind alle t-homogenen endlichen Permutationsgruppen auf n Objekten bekannt, falls $2 \le t \le \lfloor (n-1)/2 \rfloor$ ist. Nur die affinen und projektiven Gruppen liefern Serien optimaler s-PA. Spätestens für t>5,wo $A_t$ und $S_t$ die einzigen t-homogenen Gruppen sind, muß man sich etwas anderes einfallen lassen.

**(3.1) Satz**

*a) Existiert eine Gruppe G, mit einer t-fach transitiven Darstellung auf einer v-Menge V, so existiert ein $OD_\lambda(t,v,v)$ mit* $\lambda = |G|/t!\binom{v}{t}$.

*b) Existiert eine Gruppe G, mit einer t-fach homogenen Darstellung auf einer v-Menge V, so existiert ein $PA_\lambda(t,v,v)$ mit* $\lambda = |G|/\binom{v}{t}$.

*Beweis* Für $a \in V$ und $g \in G$ sei $a^g$ das Bild von a unter der Operation mit g. Sei die (v,v)-Matrix A definiert durch $A = (a_{g,v})_{g\in G, v\in V}$, wo $a_{g,v} := v^g$. Für $B \subseteq V$ und $g \in G$ sei $B^g := \left(b^g | b \in B\right)$.

a) Da G t-fach transitiv auf V operiert, gibt es nach Definition zu jedem Paar $C,D \subseteq V$ geordneter t-Mengen Elemente $g \in G$, die C auf D abbilden. Es sei $X(C,D) := \left\{ g \in G \middle| C^g = D \right\}$. Dann ist |X(C,D)| konstant, unabhängig von der Wahl des Paares C,D. Also steht in jeder t-Menge C von Spalten von A jede geordnete t-Menge D von Einträgen gleich oft, d.h. A ist ein $OD_\lambda(t,v,v)$. Mit #A=|G| und da die Anzahl der geordneten t-Mengen von V gleich $t!\binom{v}{t}$ ist, folgt die Behauptung.

b) Da G t-fach homogen auf V operiert, gibt es nach Definition zu jedem Paar $C,D \subseteq V$ ungeordneten t-Mengen Elemente $g \in G$, die C auf D abbilden. Man verfahre analog zu a). ❑

**(3.2) Folgerung** *Existiert eine Gruppe G, mit einer t-fach transitiven Darstellung auf einer v-Menge V, so existiert ein $t\text{-}PA_\lambda(t,k,v)$ mit* $\lambda = |G|/\binom{v}{t}$ *für alle $t \le k \le v$.*

*Beweis*: Nach (3.1 a) existiert unter diesen Voraussetzungen ein OD(t,v,v). Die Restriktion auf eine k-Teilmenge der Spalten ist klarerweise ein OD(t,k,v). Nach (2.11 j) folgt die Behauptung. ❑

Damit haben wir folgende Beispiele für PA (Eigenschaften der Gruppen siehe z.B. [13])

**(3.3) Folgerung**

a) *Die affine Gruppe $AGL_2(q)$ (q Primzahlpotenz) operiert scharf 2-fach transitiv auf $\mathbb{F}_q$ . Dies liefert ein 2-$PA_2(2,k,q)$, für $2\le k\le q$. Diese sind optimal als 2-PA (äquivalent zu 1-PA da t=2 siehe (2.11 f)), falls nicht k und q ungerade, und optimal als 0-PA für q= 2-Potenz.*

b) *Die Projektive Gruppe $PGL_2(q)$ (q Primzahlpotenz) operiert scharf 3-fach transitiv auf der projektiven Geraden. Dies liefert ein 3-$PA_6(3,k,q+1)$ für $3\le k\le q+1$. Diese sind optimal als 3-PA (äquivalent zu 2-PA da t=3 siehe (2.11 f)) und als 1-PA für k gerade, $q\equiv 0,2 \pmod 6$.*

c) *Die $PSL_2(q)$ ($q\equiv 3 \pmod 4$, q Primzahlpotenz) operiert 3-homogen auf der projektiven Geraden. Dies liefert ein 3-$PA_3(3,k,q+1)$ für $3\le k\le q+1$. Diese sind optimal als 3-PA (äquivalent zu 2-PA da t=3 siehe(2.11 f)), als 1-PA und als 0-PA für $q\equiv 3,11 \pmod{12}$.*

d) *Die $PSU_3(q)$ q>2 (q Primzahlpotenz) operiert 2-fach transitiv auf den $q^3+1$ Punkten des hermiteschen Unitals. Dies liefert ein 2-$PA_\lambda(2,k,q^3+1)$ für $2\le k\le q^3+1$ mit* $\lambda = \dfrac{2(q^2+1)}{ggt(3,q+1)}$

e) *Die Reegruppe R(q) ($q=3^{ungerade}$) operiert 2-fach transitiv auf den $q^3+1$ Punkten des Ree-Unitals. Dies liefert ein 2-$PA_{2(q-1)}(2,k,q^3+1)$ für $2\le k\le q^3+1$.*

f) *Die Suzukigruppen Sz(q) ($q=2^{ungerade}$) operieren 2-fach transitiv auf den $q^2+1$ Punkten des Tits-Ovoids. Dies liefert ein 2-$PA_{2(q-1)}(2,k,q^2+1)$ für $2\le k\le q^2+1$.*

*Beweis:* a), b),d)..f) Nach (3.2). Optimalität folgt aus (2.16) siehe auch Anhang A.

c) Für t=3 liefert die (3-homogene) Gruppe $PSL_2(q)$ ($q\equiv 3 \pmod 4$, q Primzahlpotenz) ein $PA_3(3,q+1,q+1)$. Auf dessen Spalten operiert nach Konstruktion $PSL_2(q)$, damit insbesondere auf jeder 3-Menge von Spalten eine $Z_3$ und auf jeder 2-Menge von Spalten eine $Z_2$. Mit einem Vorgriff auf (3.13) und dem Restriktionskriterium (2.19) erhalten wir einen 3-$PA_3(3,k,q+1)$ für $3\le k\le q+1$. Optimalität folgt aus (2.16), siehe auch Anhang A. ❑

Es gibt noch ein paar einzelne Gruppen, die PA mit kleinem λ liefern

**(3.4) Folgerung**

*$AGL_2(8)$ liefert ein $PA_1(3,8,8)$ (optimal)*

*$P\Gamma L_1(32)$ liefert ein $PA_1(3,32,32)$ (optimal)*

*$PGL_2(8)$ liefert ein $PA_4(4,9,9)$ (optimal wäre $\lambda=2$)*

*$P\Gamma L_2(32)$ liefert ein $PA_4(4,33,33)$ (optimal wäre $\lambda=2$)*

*$M_{11}$ liefert ein 3-$PA_{48}(3,k,11)$ und ein 4-$PA_{24}(4,k,11)$ ($k\ge 3$ bzw. $k\ge 4$)*

*$M_{12}$ liefert ein 4-$PA_{192}(4,k,12)$ und ein 5-$PA_{120}(5,k,12)$ ($k\ge 4$ bzw. $k\ge 5$)*

Als nächstes wollen wir versuchen, PA als Teilmengen homogener Gruppen zu finden.

Zuerst wollen wir die affine Gruppe halbieren (was wegen (2.17) natürlich nur für ungerades q möglich ist). Die zugrundeliegenden Ideen lassen sich allgemeiner formulieren.

**(3.5) Definition** *Sei* $A = (a_{i,k})_{i\in I,k\in K}, a_{i,k} \in V$ *eine (K,V)-Matrix, L eine Gruppe die auf V operiert und R eine Gruppe, die auf K operiert. Definiere für* $\sigma\in L$ *:*

$$\sigma A := (c_{i,k})_{v\in I,k\in K},\ c_{i,k} := (a_{i,k})^{\sigma} \text{ und } LA := \bigcup_{\sigma\in L} \sigma A,$$

*sowie für* $\rho\in R$*:*

$$A\rho := (c_{i,k})_{i\in I,k\in K},\ c_{i,k} := a_{i,k^{\rho}} \text{ und } AR := \bigcup_{\rho\in R} A\rho.$$

*Sind A, B (K,V)-Matrizen und läßt sich A darstellen als A=LB, so sagt man L* operiert *auf den Einträgen von A, und B heißt ein* Repräsentantensystem *von A (bzgl. L). Läßt sich A darstellen als A=BR, so sagt man R* operiert *auf den Spalten von A, und B heißt ein* Repräsentantensystem *von A (bzgl. R) .*

**(3.6) Beispiel** Auf den Spalten des PA aus Beispiel (1.2) operiert eine $Z_5$. Es läßt sich darstellen als VR, mit:

$$R := <(0,1,2,3,4)>, \quad V := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix}$$

**(3.7) Bemerkung** *Ist k=v, so kann man die Zeilen einer (v,v)-Matrix als Permutationen aus* $S_v$ *auffassen. Sei A=LVR ein* $PA_{\lambda}(t,v,v)$*, auf dessen Einträgen eine Gruppe L operiert und auf dessen Spalten eine Gruppe R operiert. Dann ist* $A^{-1}=RV^{-1}L$ *wieder ein* $PA_{\lambda}(t,v,v)$*, wobei sich die Rollen von L und R vertauscht haben. Insbesondere ist das Invertieren im Falle k=v ein Isomorphismus zwischen PA.*

*Beweis* $A^{-1}=(LVR)^{-1}=R^{-1}V^{-1}L^{-1}=RV^{-1}L$, da L, R Gruppen sind. Beim Invertieren einer Zeile z vertauschen sich die Rollen von Einträgen und Spalten: steht in z die t-Menge E von Einträgen in der t-Menge S von Spalten, so steht in $z^{-1}$ die t-Menge S von Einträgen in der t-Menge E von Spalten. Es ist zu zeigen: in $A^{-1}$ kommt die t-Menge S von Einträgen in der t-Menge E von Spalten genau $\lambda$ mal vor. Dies ist äquivalent zu: in A kommt die t-Menge E von Einträgen in der t-Menge S von Spalten genau $\lambda$ mal vor. Dies gilt, da A ein $PA_{\lambda}(t,v,v)$ ist. ❑

**(3.8) Definition** *Sei R ein Ring bzw. eine Gruppe. Eine Teilmenge* $U\subseteq R$ *heißt ein* Halbsystem *gdw* $x\in U \Leftrightarrow -x\notin U$ *für alle* $0\neq x\in R$

**(3.9) Bemerkung** *Ist R ein Ring,* $U\subseteq R$ *ein Halbsystem, e eine Einheit (*$e\in R^*$*), so ist eU ein Halbsystem.*

*Beweis:* Annahme eU wäre kein Halbsystem. Denn gäbe es ein $a\in eU$, so daß auch $-a\in eU$. Es gäbe also $x,y\in U$, so daß $a=ex$ und $-a=ey \Rightarrow ex-ey=0$. Da e Einheit folgt $x=-y$. Damit sind $y,-y\in U$. Dies ist ein Widerspruch zur Voraussetzung, daß U ein Halbsystem ist. ❑

Als erstes werde ich mich hier mit $PA_1(2,k,v)$, auf deren Einträgen eine Gruppe der Ordnung v transitiv operiert, beschäftigen. Dies wurde zum Teil schon in [20] behandelt. Dies ist als Methode der Differenzenmatrizen bekannt.

**Achtung** ich verwende wie in den ursprünglichen Arbeiten als Symbol "+" für die Verknüpfung obwohl bei mir die Gruppe nicht immer kommutativ ist.

**(3.10)Satz** *Sei (G,+) eine Gruppe ungerader Ordnung v und A,B (k,G)Matrizen,. Dann gilt:*

*a) GA ist ein $PA_1(2,k,v)$ gdw $\{a_{i,j} - a_{i,k} | i \in I\}$ ein Halbsystem von G bildet für alle $j \neq k \in K$.*

*b) Ist G kommutativ und GA ein $PA_1(2,k,v)$, so gibt es ein B, so daß $G(A \cup B)$ ein $OD_1(2,k,v)$ ist. (Man sagt: das PA ist komplementierbar)*

*c) Ist GA ein $OA_1(2,k,v)$, so läßt sich GA zu einem $OA_1(2,k+1,v)$ ergänzen.*

*d) GA ist ein $APA_1(2,k,v)$ gdw zusätzlich zu a) für jedes $j \in K$ und jedes $g \in G-\{0\}$ gilt: läuft i durch I und k durch K-{j}, so nimmt $(a_{i,j}-a_{i,k})$ den Wert g genauso oft an wie -g.*

*Beweis:* BezeichnungSei $g,h \in G$, so schreibe die Operation von G auf G (durch (rechts-) Multiplikation) als $g^h := g + h$ .

a) Zu zeigen: ein Paar (g,h) von Einträgen, kommt in den Spalten (j,k) genau einmal vor. Nach Annahme bilden die Differenzen zweier Spalten ein Halbsystem, es gibt also ein i, so daß $(a_{i,j}-a_{i,k}) = \pm(g-h)$.
Fall 1) Falls $(a_{i,j}-a_{i,k})=(g-h)$, so hat $(-a_{i,j}+g)A$ in Zeile i und Spalte j das Element $a_{i,j}-a_{i,j}+g=g$ stehen und in Zeile i und Spalte k das Element $a_{i,k}-a_{i,j}+g = -(g-h)+g = h-g+g=h$ stehen.
Fall 2) Falls $(a_{i,j}-a_{i,k}) = -(g-h)$, so hat $(-a_{i,k}+g)A$ in Zeile i und Spalte j das Element $a_{i,j}-a_{i,k}+g = -(g-h)+g=h$ stehen und in Zeile i und Spalte k das Element $a_{i,k}-a_{i,k}+g=g$ stehen.
Also kommt jedes ungeordnete Paar mindestens einmal in jedem Spaltenpaar vor. Aus Anzahlgründen dann genau einmal.

b) $(GA) \cup (G(-A)) = G(A \cup (-A))$ mit $-A = (c_{i,k})_{i \in I, k \in K}$, mit $c_{i,k} = -a_{i,k}$ ist das gesuchte OD. Falls in A:$(a_{i,j}-a_{i,k})=(g-h)$ ist, so erhält man aus der entsprechenden Zeile von -A, $(-a_{i,j}+a_{i,k}) = -(-a_{i,k}+a_{i,j}) = -(a_{i,j}-a_{i,k})$ ( da G hier kommutativ) $= -(g-h)$. Falls also bei A Fall 1) eintritt, tritt bei (-A) Fall 2) ein und umgekehrt. Somit kommt in $(GA) \cup (G(-A))$ jedes Paar in jeder Anordnung einmal vor; $(GA) \cup (G(-A))$ ist also ein $OD_1(2,k,v)$. Bemerkung: auf dem nach (1.9 b) existierenden $OA_1(2,k,v)$ operiert G natürlich auch.

c) Nach Annahme existiert ein $OA_1(2,k,v)$, der Form GA. Da #A=|G|, können wir die Zeilen von A durch G indizieren. Man füge nun zu GA eine neue Spalte hinzu, in die man, in den zu G(A(i)) korrespondierenden Zeilen, $i \in G$ einfügt. Damit hat man erreicht, daß in alle Zeilen, die in der neuen Spalte ein festes $i \in G$ stehen haben, in den anderen Spalten alle Elemente aus G durchlaufen. Also kommt in Paaren einer neuen Zeile mit einer beliebigen anderen Zeile jedes Paar aus G gleich oft vor.

d) Da nach a) GA schon ein PA ist, bleibt nur noch E(1,2) zu zeigen: in den Zeilen, die {a,b} enthalten, muß in jeder Spalte j der Eintrag a (wie auch b) gleich oft vorkommen. Also müssen Fall 1) und Fall 2) gleich oft vorkommen, wenn man k durch alle Spalten ungleich j laufen läßt, Dies führt unmittelbar auf die Bedingung in d) ❑

**(3.11) Folgerung** (Theorem 2.4 [20]) *Sei R ein Ring, |R| ungerade, U ein Halbsystem von R und I⊆R, so daß für alle j,k∈I, j≠k folgt j-k∈R*. Dann existiert ein $PA_1(2,I,R)$.*

*Beweis* Definiere $A = (a_{u,i})_{u\in U, i\in I}$ mit $a_{u,i} := ui \in R$ und verwende (3.7 a) mit R als additiver Gruppe. Für $j\neq k\in I$ gilt $\{a_{u,j} - a_{u,k} | u \in U\} = \{uj - uk | u \in U\} = U(j-k)$. Nach Voraussetzung ist j-k∈R*, damit U(j-k) nach (3.8) Halbsystem, also RA das gesuchte $PA_1(2,I,R)$. ❑

**(3.12) Folgerung** (Theorem 2 [21]) *Ist q ungerade Primzahlpotenz, so existiert ein $PA_1(2,q,q)$, das eine Halbierung des durch die $AGL_2(q)$ gewonnenen OD ist.*

*Beweis:*
Da $\mathbb{F}_q$ ein Körper ist, gilt für alle $a\neq b\in \mathbb{F}_q$, daß $a-b\in \mathbb{F}_q^*$. Also existiert nach (3.10) ein $PA_1(2, \mathbb{F}_q, \mathbb{F}_q)$. Die affine Gruppe in ihrer Operation auf dem endlichen Körper $\mathbb{F}_q$ läßt sich darstellen als $AGL_2(q)=\{(m,a)\in \mathbb{F}_q^* \times \mathbb{F}_q\}$ die auf $t\in \mathbb{F}_q$ via $(m,a): t \mapsto mt+a$ operiert. Dies ist dieselbe Konstruktion wie im Beweis von (3.10), da $\mathbb{F}_q^*=U\cup -U$ für ein beliebiges Halbsystem U von $\mathbb{F}_q$ und da $\mathbb{F}_q$ kommutativ ist. Also entspricht das OD aus (3.1 a) gerade dem, das laut (3.9 b) aus den $PA_1(2, \mathbb{F}_q, \mathbb{F}_q)$ hervorgeht. ❑

**(3.13) Satz** *Sei A ein $PA_\lambda(w,k,v)$, R eine Gruppe, die (w-u) fach-homogen auf den Spalten von A operiert. Dann hat A die Eigenschaft E(u,w).*

*Beweis:* Seien U⊆W⊆V mit |U|=u und |W|=w. Da R nur die Spalten vertauscht, bildet R jede Zeile, die W enthält, wieder auf eine solche ab. Also zerfallen die Zeilen, die W enthalten, in Bahnen unter R. Wegen der (w-u)-fachen Homogenität von R wird in der Bahn jedes Repräsentanten, W-U gleich oft in jede (w-u)-Menge von Spalten abgebildet. Die Zahl der Zeilen, die W enthalten, ist eine Konstante, da A ein $PA_\lambda(w,k,v)$ ist. Also folgt die Behauptung. ❑

**(3.14) Folgerung** *Die Situation sei wie in (3.11). Sei R ein Ring, |R| ungerade, U ein Halbsystem von R und I⊆R, so daß für alle j,k∈I, j≠k gilt j-k∈R*. Gelte zusätzlich:*

- *a) I ist eine (multiplikative) Untergruppe ungerader Ordnung von R*. Dann gibt es ein $APA_1(2,I,R)$.*
- *b) Ist I eine additive Untergruppe von R, so gibt es ein $APA_1(2,I,R)$*

*Beweis:*

a) Da |R| ungerade, gilt x≠-x für alle 0≠x∈R, somit gilt x∈I⇒-x∉I, da sonst |I| gerade. Also läßt sich I zu einem Halbsystem U, das aus Nebenklassen von I besteht, ergänzen. Insbesondere gilt dann Uk=U für alle k∈I. Man benutze dieses Halbsystem für die Konstruktion nach (3.11) und erhält ein $PA_1(2,I,R)$, das wir A nennen. $A = (a_{(u,r),i})_{u\in U\times R, i\in I}$ mit $a_{(u,r),i} = ui + r$. Die Menge I operiert transitiv auf I mittels $k^l := lk$ für $k,l \in I$. Um (3.13) anwenden zu können, muß man zeigen, daß I auf den Spalten von A operiert. Ein k∈I bildet eine Zeile $(a_{(u,r),i} | i \in I)$ von A ab auf $(a_{(u,r),ki} | i \in I) = (uki + r | i \in I) = (a_{(uk,r),i} | i \in I)$. Dies ist wieder eine Zeile von A, da uk∈U nach Konstruktion von U. Damit folgt die Behauptung, da E(1,2) nach (3.13) gilt.

b) Da |R| ungerade, ist der Teiler |I| von |R| ebenfalls ungerade. I operiert auf I transitiv mittels $k^l := k + l$ für $k,l \in I$. Man benutze (3.13) und erhalte ein $PA_1(2,I,R)$ A. Es ist $A = (a_{(u,r),i})_{u\in U\times R, i\in I}$ mit $a_{(u,r),i} = ui + r$. Ein $k\in I$ bildet eine Zeile $(a_{(u,r),i}|i \in I)$ von A ab auf $(a_{(u,r),i+k}|i \in I) = (u(i+k)+r|i \in I) = (a_{(u,uk+r),i}|i \in I)$. Dies ist wieder eine Zeile von A, da uk+r∈ R. Damit folgt die Behauptung, da E(1,2) nach (3.13) gilt. ❏

**(3.15) Folgerung** *$AGL_2(q)$ enthält ein $APA_1(2,k,q)$ falls k,q ungerade und entweder*

*a) (q)≡ 1(mod k) oder*

*b) k|q gilt.*

*Beweis*

a) Setze R= $\mathbb{F}_q$ . Also gibt es eine (multiplikative) Untergruppe K der Ordnung k von $\mathbb{F}_q^*$ (da $\mathbb{F}_q^*$ zyklisch), die Behauptung folgt mit (3.14 a). Zur Einbettung in $AGL_2(q)$ vgl. (3.12).

b) Sei K additive Untergruppe von $\mathbb{F}_q$ mit |K|=k. Die Behauptung folgt mit (3.14 b). Zur Einbettung in $AGL_2(q)$ vgl. (3.12). ❏

(3.15 a) ist die Hauptaussage der Arbeit [10], wird dort aber anders bewiesen.
(3.15 b) ist ein Fortschritt zu den Ergebnissen, die man mit den affinen Design's erhält, z.B existiert ein $APA_1(2,9,27)$.

**(3.16) Beispiel** Wir konstruieren explizit ein $APA_1(2,5,11)$, das gemäß (3.15 a) existiert. Sei K die Untergruppe der Ordnung 5 von $\mathbb{F}_{11}^*$, diese wird z.B. durch $m_3 : x \mapsto 3x$: erzeugt. Die Elemente aus K bilden, wie man aus Beweis von (3.14) ersehen kann, ein Halbsystem (da K schon die richtige Ordnung hat). Numerieren wir die Spalten fortlaufend mit 1..k so müßen wir K zu K' transformieren und erhalten:

$$K := < (1,3,9,5,4) >$$

$$K' := < (1,2,3,4,5) >$$

$$A := < (0,1,2,3,4,5,6,7,8,9,10) >$$

$$V_1 := (0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10)$$

$$V_2 := (1 \quad 3 \quad 9 \quad 5 \quad 4)$$

$AV_1K'$ ist damit nach (3.13) ein $PA_1(2,11,11)$

$AV_2K'$ ist damit nach (3.15) ein $APA_1(2,5,11)$

Wir betrachten jetzt Teilmengen der PGL(2,q) in ihrer Operation auf der projektiven Geraden

Der folgende Satz zeigt, daß wir die uniform 3-homogenen Teilmengen der PGL(2,q) schon alle kennen.

**(3.17) Satz** *Ist A eine uniform 3-homogene Teilmenge der PGL(2,q), so gilt einer der folgenden Fälle:*

*a) q=7 b) q=5,8*

*c) $q \equiv 3 \bmod 4$ und $A=PSL(2,q)$ oder deren Komplement*

*Beweis* siehe [3]

Die PSL(2,q) ist 2-fach transitiv auf der projektiven Geraden. Wir suchen nach uniform 2-homogenen Teilmengen von PSL(2,q).

**(3.18) Satz** *Genau dann wenn* $q \not\equiv 3 \pmod 4$ *ist, läßt sich die PSL(2,q) zu einem* $PA_\lambda(2,q+1,q+1)$ *halbieren, wobei* $\lambda = \begin{cases} q-1 & q \text{ gerade} \\ \frac{1}{2}(q-1) & \text{sonst} \end{cases}$

*Beweis:*

Fall $q \equiv 3 \pmod 4$: PSL(2,q) läßt sich nicht halbieren, da sonst $\lambda = (q-1)/2$ ungerade. Widerspruch zu (2.17)

Fall $q=2^f$: $PSL(2,2^f)=PGL(2,2^f)=:G$. Seien $m_\lambda, u_\gamma$ die Elemente aus G für die gilt: $\tau^{m_\lambda} = \lambda\tau$ und $\tau^{u_\gamma} = \tau + \gamma$ für $\lambda \in \mathbb{F}_q^*$ bzw. $\gamma \in \mathbb{F}_q$ und $\tau$ Element der projektiven Geraden $:= \mathbb{F}_q \cup \{\infty\}$. Sei $Z = \langle z \rangle \le G$ eine zyklische Untergruppe von G $|Z|=q+1$. Wähle z, so daß $0^z = \infty$ und $\infty^z = 1$; dies ist möglich, da PGL 3-fach transitiv ist. Jedes $g \in G$ läßt sich nun eindeutig schreiben als $g=m_\lambda u_\gamma z^i$. Definiere

$$a_i := z^i(\infty) \quad (*)$$

wobei der Index i mod (q+1) gelesen wird. Jedes Element der projektiven Geraden ist also ein $a_i$. Es gelten :

1) $a_i = a_{-i}+1$. Denn das Element $\sigma \in G$, so saß $z^\sigma = z^{-1}$ ist bis auf die Wahl des Fixpunktes eindeutig bestimmt. Wähle als Fixpunkt ∞, so kann man sich leicht überzeugen, daß das Element $u_1$ bei unserer speziellen Wahl von z ein solches ist.

2) $$(a_i, a_j)^{z^{-i-j}} := (a_i^{z^{-i-j}}, a_j^{z^{-i-j}}) = (z^{-i-j}z^i(\infty), z^{-i-j}z^j(\infty)) = (z^{-j}(\infty), z^{-i}(\infty))$$
$$= (a_{-j}, a_{-i}) \overset{1)}{=} (a_j + 1, a_i + 1)$$

Wähle $U \subseteq F$, so daß $x \in U \Leftrightarrow 1+x \notin U$. Dies liefert eine Partition von G in zwei gleich große Teile A und B, mit:

$$A = \left\{ g \in G \middle| g = m_\lambda u_\gamma z^i \text{ für } \lambda \in F^*, \gamma \in U, 0 \le i \le q \right\}$$

und B=G-A. Sei (a,b) ein Paar von Elementen der projektiven Geraden, $g=m_\lambda u_\gamma z^\nu \in G$, so ist $a^g = z^\nu(\lambda a + \gamma)$ und $b^g = z^\nu(\lambda b + \gamma)$. Nach $(*)$ gibt es i,j, so daß

$$\lambda a+\gamma = a_i \text{ und } \lambda b+\gamma = a_j.$$

Für jedes Paar (a,b) definiere die Abbildung

$$\Phi_{a,b} : m_\lambda u_\gamma z^\nu \; a \; m_\lambda u_{\gamma+1} z^{\nu+i+j}.$$

Da "$u_\gamma$ auf $u_{\gamma+1}$ abgebildet wird", bildet $\Phi_{a,b}$ ein g aus Teil A nach B ab und umgekehrt (beachte, daß die Charakteristik 2 ist). Außerdem ist $\Phi_{a,b}$ offensichtlich eine Bijektion. Es gilt:

$$(a,b)^g = (z^\nu(a_i), z^\nu(a_j))$$

$$(a,b)^{\Phi_{a,b}(g)} = (z^{\nu+i+j}(\lambda a+\gamma+1), z^{\nu+i+j}(\lambda a+\gamma+1)) = (z^{\nu+i+j}(a_i+1), z^{\nu+i+j}(a_j+1))$$

$$= (z^{\nu+i+j}(a_{-i}), z^{\nu+i+j}(a_{-j})) \overset{2)}{=} (z^\nu(a_j), z^\nu(a_i))$$

Also wird (a,b) durch g und $\Phi_{a,b}(g)$ auf dasselbe ungeordnete Paar abgebildet. Da $\Phi_{a,b}$ eine Bijektion zwischen den Teilen A und B und G 2-fach transitiv ist, gibt es in A und in B gleich viele Elemente, die (a,b) auf ein vorgegebenes ungeordnetes Paar abbilden. Damit ist die Matrix $C = (c_{a,\tau})_{a\in A,\tau\in \mathbb{F}_q \cup\{\infty\}}$ mit $c_{a,\tau} := \tau^a$ ein $PA_\lambda(2,q+1,q+1)$ mit $\lambda = \frac{|G|}{2\binom{q+1}{2}} = \frac{(q+1)q(q-1)}{(q+1)q} = q-1$.

Fall $q\equiv 1 \pmod 4$: Da $q\equiv 1 \pmod 4$ gibt es $i\in \mathbb{F}_q^*$ mit $-1=i^2$. Sei $G=PSL(2,q)$, $Z = \langle z\rangle \le G$ eine zyklische Untergruppe der Ordnung (q-1)/2, die 0 und ∞ in verschiedenen Bahnen hat. Dies ist möglich, da G eine 2-fach transitive Gruppe ist. Wähle ein Halbsystem R von $\mathbb{F}_q$ . Seien $t_\lambda, w_\lambda$ die Elemente aus G für die gilt: $\tau^{t_\lambda} = \lambda^2\tau$ und $\tau^{w_\lambda} = (\lambda^2\tau)^{-1}$, $u_\gamma$ wie im vorherigen Fall. Jedes $g\in G$ läßt sich nun eindeutig schreiben als $g=u_\gamma t_\lambda z^\nu$ oder $g=u_\gamma w_\lambda z^\nu$ mit $\lambda\in R$, $\gamma\in \mathbb{F}_q$ und $0\le\nu\le(q+1)/2$, denn angenommen, ein g hätte 2 solche Darstellungen, so müßten diese auf jedem Element der projektiven Geraden gleich operieren. Außerdem sieht man $u_\gamma x z^\nu = u_\alpha y z^\delta \Rightarrow u_\gamma x = u_\alpha y z^{\delta-\nu}$, also sind die folgenden Fälle zu betrachten:

1) $u_\alpha t_\beta = u_\gamma w_\lambda z^\nu$. Wir setzen $\tau=\infty$:

$$\infty = \beta^2\infty + \alpha = z^\nu((\lambda^2(\infty+\gamma))^{-1}) = z^\nu(0)$$

ein Widerspruch zur Wahl von 0 und ∞ in verschiedenen Bahnen von Z. Der Fall $u_\alpha w_\beta = u_\gamma t_\lambda z^\nu$ ist analog zu behandeln.

2) $u_\alpha t_\beta = u_\gamma t_\lambda z^\nu$, so setze für $\tau=\infty$:

$$\infty = \beta^2\infty + \alpha = z^\nu(\lambda^2(\infty+\gamma)) = z^\nu(\infty)$$

Da Z keine Fixpunkte hat, folgt damit $0=\nu$. Die Wahl $\tau=0$ liefert $\alpha=\gamma$, und $\tau=1$ liefert $\beta^2 = \lambda^2 \Rightarrow \beta = \pm\lambda$. Da $\beta,\lambda\in R$, folgt $\beta=\lambda$. Der Fall $u_\alpha w_\beta = u_\gamma w_\lambda z^\nu$ folgt in analoger Weise.

Sei $X\subset R$ mit $x\in X \Leftrightarrow \pm ix \notin X$. Vereinfachend bezeichnen wir das Element $t_{\pm ix}$, das zu $\pm ix\in R$ gehört als $t_{ix}$. Da beide Vorzeichen zur selben Abbildung führen besteht keine Gefahr des Mißverständnisses, insbesondere ist $t_{ii\lambda}=t_\lambda$. Damit erhält man analog zum obigen Fall eine Partition von G in zwei gleich große Teile A und B. Definiere für jedes Paar (a,b) der projektiven Geraden die Abbildung $\Phi_{a,b} : G \to G$

$$\Phi_{a,b}(g) := \begin{cases} u_{-a-b-\gamma} t_{i\lambda} z^\nu & \\ u_{-a-b-\gamma} w_{i\lambda} z^\nu & \\ u_{-2b-\gamma} t_{i\lambda} z^\nu & \text{falls} \\ u_{-2b-\gamma} w_{i\lambda} z^\nu & \\ u_{-2a-\gamma} t_{i\lambda} z^\nu & \\ u_{-2a-\gamma} w_{i\lambda} z^\nu & \end{cases} \begin{array}{ll} g = u_\gamma t_\lambda z^\nu, & a \neq \infty \neq b \\ g = u_\gamma w_\lambda z^\nu, & a \neq \infty \neq b \\ g = u_\gamma t_\lambda z^\nu, & a = \infty \\ g = u_\gamma w_\lambda z^\nu, & a = \infty \\ g = u_\gamma t_\lambda z^\nu, & b = \infty \\ g = u_\gamma w_\lambda z^\nu, & b = \infty \end{array}$$

da "$t_\lambda$ bzw. $w_\lambda$ auf $t_{i\lambda}$ bzw. $w_{i\lambda}$ abgebildet wird", liefert $\Phi_{a,b}$ eine Bijektion zwischen A und B. (beachte $-1=i^2$). Es gilt:
Falls g von der Form $u_\gamma t_\lambda z^\nu$ und $a,b \neq \infty$, so ist

$$\begin{aligned} (a,b)^{u_\gamma t_\lambda z^\nu} &= (z^\nu(\lambda^2(a+\gamma)), z^\nu(\lambda^2(b+\gamma))) \\ (a,b)^{\Phi_{a,b}(u_\gamma t_\lambda z^\nu)} &= (z^\nu(-\lambda^2(a+(-a-b-\gamma))), z^\nu(-\lambda^2(b+(-a-b-\gamma)))) \\ &= (z^\nu(\lambda^2(b+\gamma)), z^\nu(\lambda^2(a+\gamma))) \end{aligned}$$

Falls g von der Form $u_\gamma t_\lambda z^\nu$ und $a=\infty$ oder $b=\infty$, so kann man $a=\infty$ wählen und erhält

$$\begin{aligned} (a,b)^{u_\gamma t_\lambda z^\nu} &= (z^\nu(\lambda^2(a+\gamma)), z^\nu(\lambda^2(b+\gamma))) = (z^\nu(\infty), z^\nu(\lambda^2(b+\gamma))) \\ (a,b)^{\Phi_{a,b}(u_\gamma t_\lambda z^\nu)} &= (z^\nu(-\lambda^2(a+(-2b-\gamma))), z^\nu(-\lambda^2(b+(-2b-\gamma)))) \\ &= (z^\nu(\infty), z^\nu(\lambda^2(b+\gamma))) \end{aligned}$$

Analoges gilt, falls g von der Form $u_\gamma w_\lambda z^\nu$

Also wird (a,b) durch g und $\Phi_{a,b}(g)$ auf dasselbe ungeordnete Paar abgebildet. Da $\Phi_{a,b}$ eine Bijektion zwischen den Teilen A und B und G 2-fach transitiv ist, gibt es in A und in B gleich viele Elemente, die (a,b) auf ein vorgegebenes ungeordnetes Paar abbilden. Damit ist die Matrix $C = (c_{a,\tau})_{a\in A, \tau \in \mathbb{F}_q \cup \{\infty\}}$ mit $c_{a,\tau} := \tau^a$ ein $PA_\lambda(2,q+1,q+1)$ mit $\lambda = \frac{|G|}{2\binom{q+1}{2}} = \frac{(q+1)q(q-1)}{2(q+1)q} = \frac{q-1}{2}$.

❑

Die in Satz (3.18) angegebene Halbierung ist die kleinste 2-homogene Teilmenge von $PGL(2,2^f)$ (siehe [7], dort wurde die Halbierung der $PGL(2,2^f)$ für f ungerade durchgeführt.). Ebenfalls Hat Bierbrauer mittels Charaktertheorie gezeigt, daß $PSU_3(3)$ und R(3) keine optimalen $PA(2,q^3+1,q^3+1)$ enthalten, sowie daß $M_{10}$ und $PSL_2(8)$ keine echten 3- bzw. 4-homogenen Teilmengen enthalten.

**(3.19) Bemerkung**

*a) Es gibt $APA_{q-1}(2,k,q+1)$ für $q=2^f$ Primzahlpotenz, falls $k/(q+1)$ oder $k/(q-1)$*

*b) Es gibt $APA_{(q-1)/2}(2,k,q+1)$ für $q \equiv 1 \pmod 4$ Primzahlpotenz, falls $k/((q+1)/2)$ oder $k/q$*

*Beweis:* Man sieht leicht, daß eine Untergruppe von $\mathbb{F}_q^*$ bzw. von $Z_{q+1}$ im Fall a) auf den Spalten des in (3.18) konstruierten PA bzw. dessen Inversen (vgl (3.7)) operiert. Im Fall b)

gilt dasselbe für eine Untergruppe von $\mathbb{F}_q$ bzw. von $Z_{q+1}$. Vergleiche Beweis von (3.15). ❑

**(3.20) Beispiel** Sei Z:=<(∞,1,4)(0,2,3)>, M:=<(1,2,4,3)> und A:=<(0,1,2,3,4)>. Wie man sich leicht überzeugt erzeugen Z,M und A eine PSL(2,5), wobei M bzw A die multiplikative bzw additive Gruppe des Körpers $\mathbb{F}_5$ mit den Elementen {0,1,2,3,4}, ist auf dem diese PSL(2,5) operiert. Die Wurzel von -1 ist i:=2. {1,2}ist ein Halbsystem R und {1}=:X das Vertretersystem von R nach i. Die Elemente $t_1$mit $\tau^{t_\lambda} = \lambda^2\tau$ und $w_1$ mit $\tau^{w_\lambda} = (\lambda^2\tau)^{-1}$ für $\tau \in \{\infty,0,1,2,3,4\}$, werden dann repräsentiert durch:

$$t_1 = (1) \qquad \text{und} \qquad w_1 = (\infty,0)(2,3)$$

Numeriert man die Spalten der folgenden Matrizen fortlaufend mit ∞,0,1.., so erhält man die folgenden (A-)PA:

$$V_1 := \begin{pmatrix} \infty & 0 & 1 & 2 & 3 & 4 \\ 0 & \infty & 1 & 3 & 2 & 4 \end{pmatrix}$$

$ZV_1A$ ist nach (3.18) ein $PA_2(2,6,6)$

$$Z' := <(\infty,0,1)>$$

$$V_2 := \begin{pmatrix} \infty & 1 & 4 \\ 0 & 1 & 4 \end{pmatrix}$$

$AV_2Z'$ ist nach (3.19) ein $APA_2(2,3,6)$

## 3.2 Konstruktion von PA mit (Doppel-)nebenklassen

Inspiriert von den obigen Ergebnissen kann man versuchen, PA direkt als Doppelnebenklassen RVL oder Nebenklassen RV bzw. VL zu konstruieren.
So habe ich z.B. ein $PA_{q-1}(2,q^2+1,q^2+1) \subseteq P\Gamma L(2,q^2)$ der Form $Z_{\frac{q^2+1}{2}} V E_{q2}$, mit der zyklischen Gruppe $Z_{\frac{q^2+1}{2}}$ der Ordnung $(q^2+1)/2$, der elementarabelschen Gruppe $E_{q2}$ der Ordnung $q^2$ und einem Vertretersystem V, in der $P\Gamma L_2(q^2)$, für q=3,5,7,9 mit dem Computer gefunden. Diese liefern analog zu (3.19) auch $APA_{q-1}(2,k,q^2+1)$ für $k/((q^2+1)/2)$ oder $k/q^2$. Es ist mir aber noch nicht gelungen, die naheliegende Vermutung, daß dies für jede ungerade Primzahlpotenz q geht, zu beweisen. Übrigens liefert der Fall q=3 ein $PA_2(2,10,10)$ sowie ein $APA_2(2,5,10)$und ein $APA_2(2,9,10)$ (alle optimal).

Zuerst wollen wir untersuchen, welche Gruppen überhaupt operieren können.

**(3.21) Notation** *Sei R eine Gruppe die auf K operiert, C⊆K. Definiere :*

$$R(C) := \left\{ g \in R \middle| C^g = C \right\}.$$

**(3.22) Folgerung** *Sei A ein 0-$PA_\lambda(t,K,v)$ auf dessen Spalten eine Gruppe R operiert. Dann gilt :*

*a) Für jedes C⊆K gibt es ein t'-$(v,k,\lambda\frac{\binom{|C|}{t'}}{|R(C)|})$, t'=Min(|C|,t).*

*b) Für jedes $C \subseteq K$, für das R(C) x-fach homogen auf C operiert, ist* $\lambda \frac{\binom{v}{t}\binom{|C|}{w}}{\binom{v}{w}\binom{|C|}{w-u}} \in \mathbb{N}$ *für* $w-u \leq x$ *und* $w \leq t$.

*Beweis:*

a) $A_C$ ist ein t'-PA(t',C,v), auf dessen Spalten R(C) operiert. Insbesondere ist $A_C$ ein t'-(v,C,γ), auf dessen Spalten R(C) operiert. Da Operation auf den Spalten aber einen Block in denselben überführt, ist auch ein Repräsentantensystem schon ein t'-(v,C,γ). In jeder t-Menge von Spalten von $A_C$ kommt eine t'-Menge von Einträgen λ mal vor; deren gibt es $\binom{|C|}{t'}$

b) Nach (3.13) gilt: $A_C$ hat Eigenschaft E(u,w). Eine doppelte Abzählung von #A ergibt die Behauptung. ❑

Dieses kann eine Einschränkung an die operierende Gruppe darstellen. So kann z.B., kein $PA_1(2,k,15)$, $k \geq 5$ existieren auf dessen Spalten eine $Z_5$ operiert. Es müßte sonst nämlich eine Teilmenge von Spalten geben, die als Einschränkung einen $PA_1(2,5,15)$ liefert, auf dessen Spalten eine $Z_5$ operiert,. Dies liefert nach (3.22 a) einen 2-(15,5,2). Dieser existiert aber nach [19] oder [1] nicht.

Desweiteren ergeben sich folgende Bedingungen.

**(3.23) Folgerung** *Sei A ein 0-$PA_\lambda$(t,K,v) auf dessen Spalten oder Einträgen eine Gruppe G operiert. Dann gilt:*

*a) hat G eine fixe t'-Menge, so ist |G| ein Teiler von* $\lambda_A(w)$ für alle $w \leq \mathrm{Min}(t,t')$

*b) |G| teilt #A*

*Beweis:*

a) Hat L eine fixe t'-Menge, so wird die in diesen Spalten stehende t'-Menge von Einträgen |G| mal reproduziert. Also muß |G| die Anzahl des Vorkommens einer w-Menge von Einträgen in einer w-Menge von Spalten für $w \leq \mathrm{Min}(t,t')$ teilen. Analog mit vertauschten Rollen von Zeilen und Spalten.

b) klar. ❑

So ist es z.B. nicht möglich, daß eine Gruppe G gerader Ordnung auf einem $PA_2(4,9,9)$ operiert, da G dann eine $Z_2$ als Untergruppe hat, diese hat natürlich eine fixe 2-Menge, aber 2 teilt nicht λ(2)=7.

Desweiteren kann man sich bei der Suche Arbeit sparen, wenn man sich überlegt, daß man einige Annahmen ohne Einschränkung der Allgemeinheit treffen kann.

**(3.24) Folgerung** *Sei A=LXR eine (k,v)-Matrix, auf deren Einträgen eine Gruppe L und auf deren Spalten ein Gruppe R operiert und habe A bezüglich (L,R) das Repräsentantensystem X, so erhält man isomorphe Matrizen, falls man :*

*a) L beliebig in der Klasse* $\left\{\sigma^{-1}L\sigma \middle| \sigma \in S_v\right\}$ *und R beliebig in der Klasse* $\left\{\sigma^{-1}R\sigma \middle| \sigma \in S_k\right\}$ *wählt.*

*b) X beliebig in* $\left\{\sigma X\rho \middle| \sigma \in N_{S_v}(L), \rho \in N_{S_k}(R)\right\}$ *bei festem L,R wählt.*

*c) Jede Zeile X(i) von X beliebig in* $\left\{\sigma X(i)\rho \middle| \sigma \in L, \rho \in R\right\}$ *bei festem L,R wählt.*

*Beweis:*
Man kann auf den Spalten von A mit einer beliebigen Permutation aus $S_k$ und auf den Einträgen von A mit einer beliebigen Permutation aus $S_v$ operieren und erhält wieder eine zu A isomorphe (k,v)-Matrix (2.9 d).

a) Damit ist LXR isomorph zu $\sigma^{-1}L\sigma(\sigma^{-1}X\sigma')\sigma'^{-1}R\sigma'$ mit dem neuen Repräsentantensystem $\sigma^{-1}X\sigma' \quad \sigma \in S_v, \sigma' \in S_k$.

b) Da $\sigma \in N_{S_v}(L) \Rightarrow \sigma L = L\sigma$ analog für R.

c) Wahl eines Vertreters. ❑

Offensichtlich hat man in dieser Situation die folgende Äquivalenz:

**(3.25) Bemerkung** *Sei A=LXR eine (k,v)-Matrix, auf deren Einträgen eine Gruppe L und auf deren Spalten ein Gruppe R operiert, bezüglich derer A das Repräsentantensystem X hat. Genau dann ist A ein* $PA_\lambda(t,k,v)$*, wenn in X, in jeder Bahn von R auf t-Tupeln von K (Spalten), aus jeder Bahn von L auf t-Tupeln von V (Einträgen) genau* $\lambda$ *Repräsentanten vorkommen, wobei man allerdings das Vorkommen mit den zugehörigen Vielfachheiten rechnen muß, falls die Bahnen nicht regulär sind.*

Weiter kann man, um die Zahl der zu untersuchenden Möglichkeiten einzuschränken, für eine Bahn von R die Reihenfolge der Vertreter der Bahnen von L vorschreiben, oder dasselbe mit vertauschten Rollen von L und R. Weitere Annahmen sind in Einzelfällen möglich

**(3.26) Beispiel** Gesucht wird ein A:=$PA_3(3,7,7)$ mit $A=Z_7XZ_5$ $X=(x_{i,j})$.
Nach (3.19 a) kann man $Z_7$=<(1,2,3,4,5,6,7)>, $Z_5$=<(3,4,5,6,7)> wählen. Nach (3.24 c) kann man $Z_7$ dazu benutzen, $x_{i,1}=1$ und $x_{i,3}<x_{i,4}\ldots x_{i,7}$ zu setzen, sowie die obige Bemerkung dazu verwenden um $x_{i,2}$ auf zwei mögliche Werte einzuschränken ((1,2) fix unter R), nämlich mit der Bedingung, daß $(x_{i,1},x_{i,2})=(1,x_{i,2})$ in der i-ten Bahn von L auf 2-Mengen von V liegen soll. Desweiteren kann man mit (3.24 b) z.B. $(1,x_{1,2})$ festlegen, da $N_{S_7}(Z_7) = AG_2(7)$ zweifach transitiv ist. Ebenso kann man z.B. $x_{1,4}=3$ festlegen da $N_{S_7}(Z_5) \geq AG_2(5)$ auch zweifach transitiv auf den Spalten 3 bis 7 ist. Damit hat man schon folgendes Aussehen von X erzwungen:

$$X = \begin{matrix} 1 & 7 & 2 & 3 & L \\ 1 & 3/6 & 2 & L & \\ 1 & 4/5 & 2 & L & \end{matrix}$$

Den Rest erledigt ein Computer in einem Augenblick und man erhält X:

$$X = \begin{matrix} 1 & 7 & 2 & 3 & 4 & 6 & 5 \\ 1 & 3 & 2 & 4 & 7 & 6 & 5 \\ 1 & 4 & 2 & 6 & 3 & 5 & 7 \end{matrix}$$

Analog kann man auch ein A:=$PA_4$(4,8,8) mit A=$Z_7XZ_5$ gewinnen.

Auch wenn jeweils nur Teile des zu konstruierten PA dieselbe Nebenklassenkonstruktion verwenden, kann man das bisher gesagte verwenden.

**(3.27) Beispiel** Wir suchen A:=$PA_2$(2,v,v) v gerade, G regulär auf den v-1 Punkten {0..v-2} und mit einem Fixpunkt ∞. Ansatz A:=G∪GσG, σ∈$S_v$ (G kann als $G1_{Sv}G$ interpretiert werden wobei die vielfachen Zeilen zu einer zusammengefaßt werden. Ist v Primzahl, so ist das aus der $AGL_2$(v) erhaltene $PA_2$(2,v,v) von dieser Form, mit G={t→a∗t|a∈F*}und σ=(t→t+1) ). Seien $B_0$..$B_{v-1}$ die Bahnen von G auf den (ungeordneten) Tupeln (diese sind alle regulär für v gerade), $B_0$ die Bahn, die den Fixpunkt von G enthält. In G kommt in der Bahn $B_i$ von Spalten ein Vertreter derselben Bahn $B_i$ der Einträge vor.
Da G den Fixpunkt nicht bewegt, muß gelten σ(∞)≠∞. Da G von beiden Seiten operiert, hat σ o.E. die Form (0,∞)σ', σ' ∈ $S_{V-2}$.Man sieht, daß die Bedingung für die Bahn der Spalten $B_0$, sowie für die Anzahl des Vorkommens des Vertreters von $B_0$ der Einträge in allen Bahnen von Spalten erfüllt ist. Man sucht also ein σ', so daß in jeder Bahn von Spalte $B_i$ ein Vertreter von der Bahn $B_j$ einmal vorkommt, falls i=j und 2 mal sonst für 1≤i,j≤v-1. An diesem Punkt kann man mit einem Computerprogamm σ' suchen. Da nach Konstruktion G auf den Saplten der so erhaltenen PA operiert erhält man nach (3.13) auch $APA_2$(2,v-1,v). Ist v keine Primzahlpotenz, so führt die Konstruktion für v=6 und v=12 zum Erfolg. Ist v∈ {10, 14, 18, 20} so existiert kein solches $PA_2$(2,v,v). Für G:=<(0,1,...,v-2)> erhält man die folgenden Ergebnisse:

Fall v=6:

| | | | | | | |
|---|---|---|---|---|---|---|
| $\sigma_1$= | 0 | ∞ | 1 | 3 | 2 | 4 |
| $\sigma_2$= | 0 | ∞ | 1 | 3 | 4 | 2 |
| $\sigma_3$= | 0 | ∞ | 1 | 4 | 2 | 3 |
| $\sigma_4$= | 0 | ∞ | 2 | 3 | 1 | 4 |
| $\sigma_5$= | 0 | ∞ | 2 | 4 | 3 | 1 |
| $\sigma_6$= | 0 | ∞ | 3 | 1 | 2 | 4 |
| $\sigma_7$= | 0 | ∞ | 3 | 2 | 4 | 1 |
| $\sigma_8$= | 0 | ∞ | 4 | 1 | 3 | 2 |
| $\sigma_9$= | 0 | ∞ | 4 | 2 | 1 | 3 |
| $\sigma_{10}$= | 0 | ∞ | 4 | 2 | 3 | 1 |

Fall v=12:
$\sigma_1$=

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\sigma_1$= | 0 | ∞ | 3 | 8 | 9 | 1 | 4 | 2 | 6 | 1 0 | 5 | 7 |
| $\sigma_2$= | 0 | ∞ | 4 | 6 | 1 | 5 | 9 | 7 | 1 0 | 2 | 3 | 8 |
| $\sigma_3$= | 0 | ∞ | 7 | 5 | 1 0 | 6 | 2 | 4 | 1 | 9 | 8 | 3 |
| $\sigma_4$= | 0 | ∞ | 8 | 3 | 2 | 1 0 | 7 | 9 | 5 | 1 | 6 | 4 |

Übrigens erzeugen G und $\sigma_3$ bzw. G und $\sigma_4$ eine Mathieugruppe $M_{12}$.

Die für die Beispiele verwendeten Programme befinden sich im Anhang, ebenso weitere mit dem Computer gefundene (A-)PA.

# 4 Spezielle Konstruktionen für den Fall t=2

## 4.1 Produktkonstruktionen

In der Literatur, die sich mit Konstruktion von PA befaßt, wurde meist der Fall t=2, $\lambda$=1 behandelt. Das Haupthilfsmittel neben der PBD-Konstruktion (2.23), ist dabei oft die "indirect singular Product"-Konstruktion gewesen, die hier in Anlehnung an [20] dargestellt wird.

**(4.1) Definition** *Ein $OA_1(2,k,v)$ bzw. $PA_1(2,k,v)$ A enthält einen* unter-$OA_1(2,k,u)$ bzw. unter-$PA_1(2,k,u)$ *B, falls es die Einschränkung von A auf eine gewisse Zeilenmenge ist.*

**(4.2) Definition** *Ein* Incomplete Array *IA(k;V,U) $U \subseteq V$ ist eine (nicht injektive) (k,V)-Matrix A, so daß in jedem Paar von Spalten jedes geordnete Paar aus (VxV)-(UxU) genau einmal vorkommt (für |U|=0 erhalten wir ein $OA_1(2,k,V)$).*

Damit erhält man unmittelbar

**(4.3) Bemerkung** *Sei A ein $OA_1(2,k,V)$ mit unter-$OA_1(2,k,U)$ B, so ist A-B ein IA(k;V,U). Die Umkehrung gilt im allgemeinen nicht.*

**(4.4) Definition** *Seien* $A = (a_j)_{j\in J}$, $B = (b_j)_{j\in J}$ *1x|J| Matrizen. Definiere:*

$$A \otimes B := (c_j)_{j\in J} \text{ mit } c_j = (a_j, b_j)$$

*Dies ist eine 1x|J| Matrix geordneter Paare. Ist* $A = (a_{i,j})_{i\in I, j\in J}$ $B = (b_{i,j})_{i\in K, j\in J}$ *so definiere:*

$$A \otimes B := \bigcup_{\substack{i\in I \\ k\in K}} A(i) \otimes B(k).$$

**(4.5) Satz** *(indirect singular Product)*

*Existieren:*

1) *ein $PA_1(2,k,v_1)$,*
2) *ein $PA_1(2,k,v_2)$ mit einem unter-$PA_1(2,k,v_3)$,*
3) *ein IA(k;$v_2$-a,$v_3$-a),*
4) *ein $PA_1(2,k,v_1(v_3-a)+a)$,*

*so existiert ein $PA_1(2,k,v_1(v_2-a)+a)$, das ein unter-$PA_1(2,k,v_1(v_3-a)+a)$ enthält. Ist $(v_2-a)>(v_3-a)*(k-1)$, so existiert ein $PA_1(2,k,v1(v_2-a)+a)$, das ein unter-$PA_1(2,k,v_1)$ enthält. Falls das $PA_1(2,k,v_1(v_3-a)+a)$ ein unter-$PA_1(2,k,v_3)$ enthält, so gibt es ein $PA_1(2,k,v_1(v_2-a)+a)$, das ein unter-$PA_1(2,k,v_2)$ enthält, das wiederum ein unter-$PA_1(2,k,v_3)$ enthält.*

Zusatz *a) Wenn eine Gruppe R auf den Spalten der PA bzw. des IA aus 1),..,4) operiert, dann auch auf dem "Produkt", und dessen unter-PA.*

*b) Wenn die PA aus 1), 2) und 4) komplementierbar sind, dann auch das "Produkt", und dessen unter-PA.*

*c) Wenn die PA aus 1), 2) und 4) APA sind, dann auch das "Produkt", und dessen unter-PA.*

*Beweis:* Sei A={a,b,...} mit |A|=($v_2$-$v_3$), Ω={α,β,...} mit |Ω|=($v_3$-a), F={$\infty_{1,...,}\infty_a$} mit |F|=a und $V_1$={1,2,..$v_1$} mit |$V_1$|=$v_1$ .Sei

$$T := \begin{pmatrix} 1 & \text{L} & 1 \\ \text{M} & & \text{M} \\ v_1 & \text{L} & v_1 \end{pmatrix}_{v_1 \times k}$$

X:=IA(k;A∪Ω,Ω)⊗$PA_1$(2,k,$V_1$)

Y'=($PA_1$(2,k,A∪Ω∪F)-$PA_1$(2,k,Ω∪F))⊗T

Z=$PA_1$(2,k,F∪(Ω×$V_1$)).

Sei Y die Matrix, die man aus Y' erhält, indem man jedes Paar ($\infty_\iota$,j) durch das entsprechende Element $\infty_\iota$ ersetzt, dann ist W:=X+Y+Z ein $PA_1$(2,k,$v_1$($v_2$-a)+a) auf der Menge der Einträge F∪((Ω∪A)×$V_1$). Die nachfolgende Tabelle zeigt, welches Paar von Einträgen in X,Y bzw. Z steht. In ihr kann man nachprüfen, daß jedes Paar genau einmal vorkommt (m,n bezeichnen Elemente aus $V_1$).

| | | |
|---|---|---|
| {(a,m),(a,n)} | m≠n | X |
| {(a,m),(b,n)} | m≠n,a≠b | X |
| {(a,m),(α,n)} | m≠n | X |
| {(a,m),(b,m)} | a≠b | Y |
| {$\infty_\iota$,(a,n)} | | Y |
| {(a,m),(α,m)} | | Y |
| {(α,m),(α,n)} | m≠n | Z |
| {(α,m),(β,n)} | m≠n,α≠β | Z |
| {(α,m),(β,m)} | α≠β | Z |
| {$\infty_\iota$,(α,n)} | | Z |
| {$\infty_i$,$\infty_j$} | i≠j | Z |

Nun betrachten wir die unter-PA in W.

Z ist ein unter-$PA_l$(2,k,$v_1$($v_3$-a)+a).

Ist ($v_2$-a)>($v_3$-a)*(k-1), so gibt es in den IA(k;A∪Ω,Ω) eine Zeile B', deren Elemente alle aus A sind. Durch Vertauschen der Elemente und der Spalten kann man ein IA(k;A∪Ω,Ω) erhalten, das eine Zeile B der Form [a..a] enthält für ein a∈ A. Dann ist B⊗$PA_1$(2,k,$v_1$) ein unter-$PA_l$(2,k,$v_1$).

Falls das unter-$PA_l$(2,k,$v_1$($v_3$-a)+a) ein unter-$PA_l$(2,k,$v_3$) enthält, so verwende man es o.E. als das in der Konstruktion verwendete $PA_1$(2,k,F∪(Ω×1)). Sei U'=($PA_1$(2,k,A∪Ω∪F)\$PA_1$(2,k,Ω∪F))⊗(1..1), und sei U die Matrix, die man aus U' erhält, wenn man jedes Paar ($\infty_\iota$,j) durch das entsprechende Element $\infty_\iota$ ersetzt. Dann ist U+$PA_1$(2,k,F∪(Ω×1)) ein unter-$PA_l$(2,k,$v_2$) das ein unter-$PA_l$(2,k,$v_3$) enthält.

Zusatz Ich beweise hier nur, daß das Produkt die geforderten Eigenschaften hat. Mit Hilfe der dadurch gelieferten Hinweise überlegt man sich leicht, daß das auch für die unter-PA gilt.

a) R operiert auf den Spalten zweier Matrizen A,B, d.h. mit A(i) ist auch $A(i)^r$ für $r \in R$ eine Zeile von A, analog für B. Damit ist auch $(A(i)\otimes B(j))^r=(A(i)^r\otimes B(j)^r)$ wieder eine Zeile von A⊗B, also operiert R auf den Spalten von A⊗B, und somit auf dem obigen X. Klarerweise operiert R auf A-B. Da jede Gruppe auf den Spalten von T operiert, operiert R damit auf Y'=(A-B)⊗T. Benennt man nun einen Teil der Einträge um, so operiert R klarerweise weiterhin auf den Spalten, damit operiert R auf Y. Auf Z operiert R nach Voraussetzung, damit auch auf W=X+Y+Z.

b) Wie man sich leicht überzeugen kann, funktioniert die obige Konstruktion genauso, wenn man alle auftretenden PA durch entsprechende OD ersetzt. Man komplettiere die gegebenen PA zu OD und führe obige Konstruktion durch. Das so erhaltene OD enthält nach Konstruktion das gesuchte PA, also ist dieses komplementierbar.

c) Sei $a,b \in F \cup ((\Omega \cup A)\times V_1)$, A die Teilmatrix von W, die aus allen Zeilen besteht, die {a,b} enthalten. Nach Konstruktion liegt A dann völlig in einem der Teile X,Y oder Z. Zu zeigen: In jeder Spalte von A kommt a gleich oft vor. Liegt A in Z, so ist dies erfüllt, da Z ein APA ist. Auch in Y folgt dies direkt aus der APA-Eigenschaft des $APA_1(2,k,A\cup\Omega\cup F)$, wenn man diese einzeln für jedes mögliche Urbild {a',b'} von {a,b} unter $Y'\rightarrow Y$ anwendet, denn {a',b'} liegt nicht im unter-$APA_1(2,k,\Omega\cup F)$, sonst läge {a,b} nicht in Y und durch die Tensorierung mit einer Zeile von T erhält man konstante erste Komponenten in jedem Eintrag. Liegt A in X, sei $a\rightarrow a'$ die Einschränkung des Tensorproduktes auf die zweite Komponente. Die Zeilen des $APA_1(2,k,V_1)$, die {a',b'} enthalten, bilden eine Untermatrix A'. In diesen kommt a' in jeder Spalte gleich oft vor (APA). Da A in X liegt, gibt es zu jeder Zeile A'(i) von A' eine Zeile $IA_{A(i)}$ des $IA(k;A\cup\Omega,\Omega)$, so daß $A = \bigcup_i IA_{A'(i)} \otimes A'(i)$, also kommt a in jeder Zeile von A gleich oft vor (a' wird in den Zeilen, die zu A gehören, nur zu a ergänzt, da 1. a in jeder Zeile von A nach Konstruktion vorkommt und 2. die zweite Komponente des Tensorproduktes injektiv ist, da es ein PA ist.). Da W ein PA, reicht die Aussage "a kommt in jeder Zeile von A gleich oft", denn man kann dann die Anzahl des Vorkommens bestimmen. Dies ist eine Konstante, unabhängig von {a,b}. Also ist W ein APA. ❑

Es ergeben sich unmittelbar folgende Spezialfälle aus (4.5).

**(4.6) Folgerungen**

x*a) Für $v_3$=a erhalten wir das direct singular Product:*

*Existieren*

1) *$PA_1(2,k,v_1)$*
2) *$PA_1(2,k,v_2)$ mit einem unter $PA_1(2,k,v_3)$*
3) *$OA_1(2,k,v_2\text{-}v_3)$,*

*so existiert ein $PA_1(2,k,v_1(v_2\text{-}v_3)+v_3)$, das ein unter-$PA_1(2,k,v_2)$ enthält, das wiederum ein unter-$PA_1(2,k,v_3)$ enthält, als auch ein unter-$PA_1(2,k,v_1)$.*

*b) Für $v_3$=a und sind die vorkommenden PA komplementierbar, so erhalten wir:*

*Existieren*

1) *$PA_1(2,k,v_1)$*

*2) $PA_1(2,k,v_2)$ mit einem unter $PA_1(2,k,v_3)$*

*so existiert ein $PA_1(2,k,v_1(v_2-v_3)+v_3)$, das ein unter-$PA_1(2,k,v_2)$ enthält, das wiederum ein unter-$PA_1(2,k,v_3)$ enthält, als auch ein unter-$PA_1(2,k,v_1)$. Alle diese sind komplementierbar.*

*c) Für $v_3=a=0$ erhalten wir:*

*Existieren*

*1) $PA_1(2,k,v_1)$*

*2) $PA_1(2,k,v_2)$*

*3) $OA_1(2,k,v_2)$,*

*so existiert ein $PA_1(2,k,v_1v_2)$, das sowohl ein unter-$PA_1(2,k,v_2)$, als auch ein unter-$PA_1(2,k,v_1)$ enthält.*

*d) Ist $v_3=a=0$ und sind die vorkommenden PA komplementierbar, so erhalten wir:*

*Existieren*

*1) $PA_1(2,k,v_1)$*

*2) $PA_1(2,k,v_2)$,*

*so existiert ein $PA_1(2,k,v_1v_2)$, das sowohl ein unter-$PA_1(2,k,v_2)$, als auch ein unter-$PA_1(2,k,v_1)$ enthält. Alle diese sind komplementierbar.*

**(4.7) Folgerungen**
*Sei $q_1...q_e=v$ die Zerlegung von v in Primzahlpotenzen mit $q_1.<...<q_e$, dann gibt es ein $PA_1(2,q_1.,v)$*
*Insbesondere existieren*
*$PA_1(2,3,v)$ für alle ungeraden $v\geq 3$*
*$PA_1(2,4,v)$ für alle ungeraden $v\geq 4$ und falls nicht 3 genau v teilt.*
*$PA_2(2,4,v)$ für alle $v\geq 4$ und falls nicht 2 oder 3 genau v teilen.*
*$PA_1(2,5,v)$ für alle ungeraden $v\geq 5$ und falls nicht 3 genau v teilt*

*Beweis:* Die $PA_1(2,k,q_i)$ sind komplementierbar (siehe (3.12)). Verwende (4.6 d) oder (2.23) mit dem 2-$(v,\{q_1,...,q_e\},1)$. ❑

**(4.8) Beispiel** Ein $PA_1(2,5,v)$, das durch die obige Folgerung nicht erfaßt wird, erhält man z.B. für $v=111=3*37$. Da wir in (3.12) gesehen haben, daß die $PA_1(2,k,q)$ (q Primzahlpotenz) komplementierbar sind und ein (unter-)$PA_1(2,k,v)$ für $v<k$ die leere Matrix ist (2.5 a), erhalten wir mit (4.6 b) ein $PA_1(2,5,111)$ indem wir $v_1=5$, $v_2=23$ und $v_3=1$ setzen, da $111= 5(23-1)+1$.

## 4.2 (nested) Steiner n-Cycle Systems

**(4.9) Definition** *Ein* n-Zykelsystem *CS(v,n) der Ordnung v, CS(v,n) ist eine Partition der Kantenmenge des vollständigen Graphen $K_v$ auf v Punkten in Kreise der Länge n. Ein CS(v,n) ist* nested, *falls man zu jedem Kreis einen Punkt (aus $K_v$) hinzufügen kann und eine Partition der Kanten des $2K_v$ in Räder mit Speichen erhält, wobei der Kreis die Felge und der zusätzliche Punkt die Nabe ist*

*Ein* Steiner n-Zykelsystem *der Ordnung v, SCS(v,n) ist ein CS(v,n) mit der zusätzlichen Eigenschaft, daß für jedes k, 1≤k≤n/2 gilt: jedes Paar von Punkten hat die Distanz k in genau einem Kreis.*

**(4.10) Bemerkung** *Existiert ein nested CS(v,n), dann ist v≡1(mod 2n)*

*Beweis:* Da die Kreise eines CS(k,v) eine Partition der Kanten des $K_v$ sind, so kommt jede Ecke in diesen Kreisen gleich oft vor. Da die Kanten der Räder eine Zerlegung des $2K_v$, sind kommt jede Ecke als Nabe gleich oft vor. Sei diese Zahl gleich t. Deshalb gilt v∗t=# der Räder $= 1/n \cdot \binom{v}{2}$ also t=(v-1)/2n damit v≡1(mod 2n). ❑

**(4.11) Satz** *Ein SCS(v,n) ist äquivalent zu einem $PA_1(2,n,v)$, auf dessen Spalten eine zyklische Gruppe der Ordnung n operiert.*

*Beweis:* Man ordne jeden Kreis eine Zeile des PA und deren zyklischen Bilder zu. Eine Kante entspricht einem Paar von Einträgen. Diese liegt in einem Kreis, falls sie in der zugehörigen Nebenklasse des PA liegt. Die "Steiner Bedingung" liefert gerade, daß jedes Eintragspaar genau einmal in jedem Spaltenpaar vorkommt (Injektivität der Zeilen folgt aus der Konstruktion). Die Konstruktion in der umgekehrten Richtung ist offensichtlich. ❑

**(4.12) Definition** *Ein zyklisches PA heißt* nested, *falls das zugehörige SCS nested ist, ein nested $PA_1(2,k,v)$ läßt sich zu einem $PA_1(2,k+1,v)$ erweitern.*

**(4.13) Satz (**Theorem 2.1 [10]) *Ist k ungerade v prim und v≡1(mod 2k) so existiert ein nested $APA_1(2,k,v)$*

*Beweis:* Siehe (3.15 a). Da k ungerade ist die Bedingung v≡1(mod 2k) äquivalent zu k und v ungerade und v≡1(mod k). Für die zusätzliche Spalte der nested Erweiterung nehme zu K in (3.15 a) noch {0} hinzu. Man überzeugt sich leicht, daß das damit erhaltene $PA_1(2,k+1,v)$ die gewünschte Eigenschaft hat. ❑

Eine weitere Besonderheit des Falles t=2 ist, daß es den Satz von Wilson gibt, der besagt, daß die notwendigen Bedingungen für die Existenz eines 2-(v,K,1) für genügend große v auch hinreichend sind. Genauer:

**(4.14) Satz** (Wilson [33]) *Sei* $K \subseteq \mathbb{N}$. *Definiere:* $\alpha(K):=ggt(k-1|k\in K)$, $\beta(K):=ggt(k(k-1)|k\in K)$. *Dann gibt es ein* $c_K \in \mathbb{N}$, *so daß aus* $v\geq c_K$, $(v-1)\equiv 0(mod\,\alpha(K))$ *und* $v(v-1)\equiv 0(mod\,\beta(K))$, *die Existenz eines 2-(v,K,1) folgt.*

Mit dem Satz von Wilson und der PBD-Konstruktion lassen sich viele Aussagen über PA(2,k,q) und APA(2,k,q) die man für Primzahlpotenzen q hat, auch für genügend große v zeigen, z.B: Satz (4.16). Für den Beweis benötigen wir noch folgenden

**(4.15) Bemerkung** (Lemma 3.4 [10]) *Für jedes gerade* $m \in \mathbb{N}$ *gibt es p und q für die gilt,* $p\equiv q\equiv 1(mod\ m)$ *und* $ggt(\,p(p-1),\,q(q-1)\,)=m$.

*Beweis* Nach Dirichlet's Satz über Primzahlen in arithmetischen Progressionen kann man $p\equiv m+1(mod\ m^2)$ wählen beachte dann gilt sowohl p≡1(mod m) als auch (p-1)/m ≡1(mod m). Somit ist ggt(p(p-1)/m,m)=1, damit läßt sich nach dem Chinesischen Restsatz

ein $r \in \mathbb{N}$ wählen mit $r \equiv 1 \pmod{m}$ und $r \equiv -1 \pmod{p(p-1)/m}$. Wieder mit dem Satz von Dirichlet läßt sich q so wählen, daß $q \equiv r \pmod{p(p-1)}$, damit ist $q \equiv 1 \pmod{m}$. Es bleibt noch zu zeigen, daß $ggt(p(p-1), q(q-1)) = m$.
Es sind $q \equiv r \equiv -1 \pmod{p(p-1)/m}$, damit ist $q(q-1) \equiv 2 \pmod{p(p-1)/m}$, aber es ist $p \equiv (p-1)/m \equiv 1 \pmod{m}$ also $p(p-1)/m$ ungerade. Damit ist $ggt(q(q-1), p(p-1)/m) = 1$. Wegen $q \equiv 1 \pmod{m}$ ist dann $ggt(p(p-1), q(q-1)) = m$. ❑

**(4.16) Satz** (Theorem 3.5 [10]) *Für jedes ungerade* $v \in \mathbb{N}$ *gibt es ein* $c_v \in \mathbb{N}$, *so daß für* $v \geq c_v$. *gilt : Es gibt ein nested* $APA_1(2,k,v)$ *genau dann wenn* $v \equiv 1 \pmod{2k}$.

Beweis: nach Bemerkung (4.15) gibt es Primzahlen p,q, so daß $p \equiv q \equiv 1 \pmod{2k}$ und $ggt(p(p-1), q(q-1)) = 2k$. Nach dem Satz von Wilson gibt es dann ein $c_v$ so daß für alle $v \geq c_v$. es dann ein 2-$(v,\{p,q\},1)$ gibt wenn $v \equiv 1 \pmod{2k}$ (da $\alpha(K) = \beta(K) = 2k$). Da $p,q \equiv 1 \pmod{2k}$ Primzahlen gibt es nach (4.13) nested $APA_1(2,k,p)$ und nested $APA_1(2,k,q)$. mit (2.23) ehalten wir dann ein $APA_1(2,k,v)$. Bemerkung (4.10) besagte, daß die Vorrausetzung $v \equiv 1 \pmod{2k}$ notwendig ist. ❑

In [23] werden alle nested SCS(v,3) die die notwendige Bedingung erfüllen konstruiert. In [19] werden alle möglichen SCS(v,5) konstruiert. Diese existieren genau für $v \equiv 1,5 \pmod{10}$ außer im Fall v=15, wo kein solches existiert.

# Anhang

# Anhang A $\mu_s(t,k,v)$ für kleine t

## $\mu_0(t, v)$ für t=2...8

| $\mu_0(2, v)$ | v (mod 2) |
|---|---|
| 1 | 1 |
| 2 | 0 |

| $\mu_0(3, v)$ | v (mod 3) |
|---|---|
| 1 | 2 |
| 3 | 0, 1 |

| $\mu_0(4, v)$ | v (mod 12) |
|---|---|
| 1 | 3, 11 |
| 2 | 5, 9 |
| 3 | 7 |
| 4 | 0, 2, 6, 8 |
| 6 | 1 |
| 12 | 4, 10 |

| $\mu_0(5, v)$ | v (mod 20) |
|---|---|
| 1 | 4, 19 |
| 2 | 9, 14 |
| 5 | 0, 3, 7, 8, 11, 12, 15, 16 |
| 10 | 1, 2, 5, 6, 10, 13, 17, 18 |

| $\mu_0(6, v)$ | v (mod 60) |
|---|---|
| 1 | 5, 29, 35, 59 |
| 2 | 20, 44 |
| 3 | 9, 15, 19, 25, 39, 45, 49, 55 |
| 4 | 14, 50 |
| 5 | 11, 17, 23, 41, 47, 53 |
| 6 | 0, 4, 24, 40 |
| 10 | 8, 32, 56 |
| 12 | 10, 30, 34, 54 |
| 15 | 1, 37, 13, 21, 27, 31, 33, 37, 43, 51, 57 |
| 20 | 2, 26, 38 |
| 30 | 12, 16, 28, 36, 48, 52 |
| 60 | 6, 18, 22, 42, 46, 58 |

| $\mu_0(7, v)$ | v (mod 105) |
|---|---|
| 1 | 6, 20, 41, 69, 90, 104 |
| 3 | 34, 55, 76 |
| 5 | 27, 48, 62, 83 |
| 7 | 0, 5, 9, 11, 14, 15, 21, 24, 26, 29, 30, 35, 36, 39, 44, 45, 50, 51, 54, 56, 59, 60, 65, 66, 71, 74, 75, 80, 81, 84, 86, 89, 95, 96, 99, 101 |
| 15 | 13, 97 |
| 21 | 1, 4, 10, 16, 19, 25, 31, 40, 46, 49, 61, 64, 70, 79, 85, 91, 94, 100 |
| 35 | 2, 3, 8, 12, 17, 18, 23, 32, 33, 38, 42, 47, 53, 57, 63, 68, 72, 77, 78, 87, 92, 93, 98, 102 |
| 105 | 7, 22, 28, 37, 43, 52, 58, 67, 73, 82, 88, 103 |

| $\mu_0(8, v)$ | v (mod 280) |
|---|---|
| 1 | 7, 55, 111, 119, 167, 175, 231, 279 |
| 2 | 27, 35, 91, 139, 147, 195, 251, 259 |
| 4 | 21, 41, 49, 69, 77, 97, 105, 125, 161, 181, 189, 209, 217, 237, 245, 265 |
| 5 | 63, 223 |
| 7 | 15, 31, 39, 47, 71, 79, 87, 95, 127, 135, 151, 159, 191, 199, 207, 215, 239, 247, 255, 271 |
| 8 | 0, 6, 14, 20, 34, 42, 56, 62, 70, 76, 84, 90, 104, 112, 126, 132, 140, 146, 154, 160, 174, 182, 196, 202, 210, 216, 224, 230, 244, 252, 266, 272 |
| 10 | 83, 203 |
| 14 | 11, 19, 51, 59, 67, 75, 99, 107, 115, 131, 155, 171, 179, 187, 211, 219, 227, 235, 267, 275 |
| 20 | 13, 133, 153, 273 |
| 28 | 1, 5, 9, 17, 25, 29, 37, 45, 57, 61, 65, 81, 85, 89, 101, 109, 117, 121, 129, 137, 141, 145, 149, 157, 165, 169, 177, 185, 197, 201, 205, 221, 225, 229, 241, 249, 257, 261, 269, 277 |
| 35 | 23, 103, 143, 183, 263 |
| 40 | 28, 48, 98, 118, 168, 188, 238, 258 |
| 56 | 2, 4, 10, 12, 16, 22, 24, 26, 30, 32, 36, 40, 44, 46, 50, 52, 54, 60, 64, 66, 72, 74, 80, 82, 86, 92, 94, 96, 100, 102, 106, 110, 114, 116, 120, 122, 124, 130, 134, 136, 142, 144, 150, 152, 156, 162, 164, 166, 170, 172, 176, 180, 184, 186, 190, 192, 194, 200, 204, 206, 212, 214, 220, 222, 226, 232, 234, 236, 240, 242, 246, 250, 254, 256, 260, 262, 264, 270, 274, 276 |
| 70 | 3, 43, 123, 163, 243 |
| 140 | 33, 53, 73, 93, 113, 173, 193, 213, 233, 253 |
| 280 | 8, 18, 38, 58, 68, 78, 88, 108, 128, 138, 148, 158, 178, 198, 208, 218, 228, 248, 268, 278 |

## $\mu_s$(t, k,v) für t=2...4, s=1..t

| $\mu_1$(2, k, v) | (k, v) (mod 2) |
|---|---|
| 1 | (1, 1) |
| 2 | sonst |

| $\mu_1$(3, k, v) | (k, v) (mod 6) |
|---|---|
| 1 | (2, 2), (5, 2), (5, 5) |
| 2 | (2, 5) |
| 3 | (k, 0), (k, 4), (1, v), (3, v), (0, 2), (2, 4), (4, 2), (5, 1), (5, 3) |
| 6 | (0, 1), (0, 3), (0, 5), (2, 1), (2, 3), (4, 1), (4, 3), (4, 5) |

$\mu_3(3, k, v)=\mu_2(3, k, v)=\mu_1(3, k, v)$

| $\mu_1$(4, k, v) | (k, v) |
|---|---|
| 1 | (3, 3), (7, 3), (11, 3), (11, 11) (mod 12) |
| 2 | (1, 3), (1, 9), (3, 9), (5, 3), (5, 5), (5, 9), (5, 11), (7, 9), (9, 3), (9, 9), (11, 5), (11, 9) (mod 12) |
| 3 | (3, 7), (3, 11), (7, 7), (7, 11), (11, 7) (mod 12) |
| 4 | (v, 0), (0, 3), (2, 2), (2, 3), (2, 5), (4, 3), (5, 2) (mod 6) |
| 6 | (1, 1), (1, 5), (1, 7), (1, 11), (3, 1), (3, 5), (5, 1), (5, 7), (7, 1), (7, 5), (9, 1), (9, 5), (9, 7), (9, 11), (11, 1) (mod 12) |
| 12 | (k, 4), (0, 1), (0, 2), (0, 5), (1, 2), (2, 1), (3, 2), (4, 1), (4, 2), (4, 5), (mod 6) |

| $\mu_2$(4, k, v) | (k, v) |
|---|---|
| 1 | (3, 3), (11, 3), (11, 11) (mod 12) |
| 2 | (3, 9), (5, 3), (5, 5), (5, 9), (5, 11), (9, 3), (9, 9), (11, 5), (11, 9) (mod 12) |
| 3 | (3, 7), (3, 11), (7, 3), (7, 7), (7, 11), (11, 7) (mod 12) |
| 4 | (0, 0), (0, 3), (2, 0), (2, 2), (2, 3), (2, 5), (3, 0), (5, 0), (5, 2) (mod 6) |
| 6 | (1, 1), (1, 3), (1, 5), (1, 7), (1, 9), (1, 11), (3, 1), (3, 5), (5, 1), (5, 7), (7, 1), (7, 5), (7, 9), (9, 1), (9, 5), (9, 7), (9, 11), (11, 1) (mod 12) |
| 12 | (k, 4), (4, v), (0, 1), (0, 2) (0, 5), (1, 0), (1, 2), (2, 1), (3, 2) (mod 6) |

$\mu_4(4, k, v)=\mu_3(4, k, v)=\mu_2(4, k, v)$

| $\mu_1(5, k, v)$ | (k, v) |
|---|---|
| 1 | v≡4, 24 (mod 60) und k≡4 (mod 5) ; v≡19, 39 (mod 60) und k≡19 (mod 20) ; v≡44 (mod 60) und k≡14 (mod 15) ; v≡59 (mod 60) und k≡59 (mod 60) |
| 2 | v≡9, 49 (mod 60) und k≡9 (mod 10) ; v≡14 (mod 60) und k≡14 (mod 15) ; v≡19, 39 (mod 60) und k≡9 (mod 20) ; v≡34, 54 (mod 60) und k≡4 (mod 5) ; v≡59 (mod 60) und k≡29 (mod 60) |
| 3 | v≡44 (mod 60) und k≡4, 9 (mod 15) ; v≡59 (mod 60) und k≡19, 39 (mod 60) |
| 4 | v≡9, 19 (mod 30) und k≡4 (mod 10) ; v≡29 (mod 30) und k≡14 (mod 30) |
| 5 | v≡0, 4 (mod 12) ; v≡3, 7 (mod 12) und k≡3 (mod 4); v≡8 (mod 12) und k≡2 (mod 3) ; v≡11 (mod 12) und k≡11 (mod 12) **mit Ausnahme der Werte (k,v) für die $\mu_1(5, k, v)=1$** |
| 6 | v≡14 (mod 60) und k≡4, 9 (mod 15) ; v≡29 (mod 60) und k≡9, 19 (mod 30) ; v≡59 (mod 60) und k≡9, 49 (mod 60) |
| 10 | v≡1, 9 (mod 12) und k≡1 (mod 2) ; v≡2 (mod 12) und k≡2 (mod 3) ; v≡3, 7 (mod 12) und k≡1 (mod 4) ; v≡6, 10 (mod 12) ; v≡11 (mod 12) und k≡9 (mod 12) **mit Ausnahme der Werte (k,v) für die $\mu_1(5, k, v)=2$** |
| 12 | v≡29 (mod 30) und k≡4, 24 (mod 30) |
| 15 | v≡8 (mod 12) und k≢0 (mod 4) ; v≡11 (mod 12) und k≡3, 7 (mod 12) **mit Ausnahme der Werte (k,v) für die $\mu_1(5, k, v)=3$** |
| 20 | ≡1, 3 (mod 6) und k≡0 (mod 2) ; v≡5 (mod 6) und k≡2 (mod 6) **mit Ausnahme der Werte (k,v) für die $\mu_1(5, k, v)=4$** |
| 30 | v≡2 (mod 12) und k≢2 (mod 3) ; v≡5 (mod 12) und k≡1, 3 (mod 6) ; v≡11 (mod 12) und k≡1 (mod 6) **mit Ausnahme der Werte (k,v) für die $\mu_1(5, k, v)=6$** |
| 60 | v≡5 (mod 6) und k≡0, 4 (mod 6) **mit Ausnahme der Werte (k,v) für die $\mu_1(5, k, v)=12$** |

| $\mu_2(5, k, v)$ | (k, v) |
|---|---|
| 1 | v≡4 (mod 60) und k≡4, 19 (mod 20) ; v≡19 (mod 60) und k≡19 (mod 20) ;<br>v≡24 (mod 60) und k≡24, 39, 44, 59 (mod 60) ; v≡39 (mod 60) und k≡39, 59 (mod 60)<br>v≡44 (mod 60) und k≡44, 59 (mod 60) ; v≡59 (mod 60) und k≡54 (mod 60) ; |
| 2 | v≡4 (mod 60) und k≡9, 14 (mod 20) ; v≡9 (mod 60) und k≡9, 29 (mod 30) ;<br>v≡14 (mod 60) und k≡14, 29 (mod 30) ; v≡19 (mod 60) und k≡9 (mod 20) ;<br>v≡24 (mod 60) und k≡9, 14, 29, 54 (mod 60) ; v≡29 (mod 60) und k≡29 (mod 30) ;<br>v≡34 (mod 60) und k≡4 (mod 5) ; v≡39 (mod 60) und k≡9, 29 (mod 60) ;<br>v≡44 (mod 60) und k≡14, 29 (mod 60) ; v≡49 (mod 60) und k≡9 (mod 10) ;<br>v≡54 (mod 60) und k≡9, 14, 24, 29 (mod 30) ; v≡59 (mod 60) und k≡59 (mod 60) |
| 3 | v≡24 (mod 60) und k≡4, 19 (mod 60) ; v≡39 (mod 60) und k≡19 (mod 60)<br>v≡44 (mod 60) und k≡4, 19, 24, 39 (mod 60) ; v≡59 (mod 60) und k≡19, 59 (mod 60) |
| 4 | v≡9 (mod 30) und k≡14, 24 (mod 30) ; v≡19 (mod 30) und k≡4 (mod 10) ;<br>v≡29 (mod 30) und k≡14 (mod 30) |
| 5 | v≡0,4 (mod 12) und k≡0, 3, 8, 11 (mod 12); v≡4 (mod 12) und k≡4, 7 (mod 12);<br>v≡7 (mod 12) und k≡3 (mod 4) ; v≡3 (mod 12) und k≡3, 11 (mod 12) ;<br>v≡8 (mod 12) und k≡8, 11 (mod 12) ; v≡11 (mod 12) und k≡11 (mod 12)<br>**mit Ausnahme der Werte (k,v) für die $\mu_2(5, k, v)=1$** |
| 6 | v≡9 (mod 60) und k≡19 (mod 30) ; v≡14 (mod 60) und k≡4, 9 (mod 15) ;<br>v≡24 (mod 60) und k≡34, 49 (mod 60) ; v≡29 (mod 60) und k≡9, 19 (mod 30) ;<br>v≡39 (mod 60) und k≡49 (mod 60) ; v≡44 (mod 60) und k≡9, 34, 49, 54 (mod 60) ;<br>v≡54 (mod 60) und k≡4 (mod 15) ; v≡59 (mod 60) und k≡9, 49 (mod 60) |
| 10 | v≡0 (mod 12) und k≡2, 5, 6, 9 (mod 12) ; v≡1 (mod 12) und k≡1 (mod 2) ;<br>v≡2 (mod 12) und k≡2, 5 (mod 6) ; v≡3 (mod 12) und k≡5, 7 (mod 12) ;<br>v≡4 (mod 12) und k≡1, 2 (mod 4) ; v≡5 (mod 12) und k≡5 (mod 6) ;<br>v≡6 (mod 12) und k≡0, 2 (mod 3) ; v≡7 (mod 12) und k≡1 (mod 4) ;<br>v≡8 (mod 12) und k≡2, 5 (mod 12) ; v≡9 (mod 12) und k≡3, 5 (mod 6) ;<br>v≡10 (mod 12) ; v≡11 (mod 12) und k≡5 (mod 12) ;<br>**mit Ausnahme der Werte (k,v) für die $\mu_2(5, k, v)=2$** |
| 12 | v≡9 (mod 30) und k≡4 (mod 30) ; v≡29 (mod 30) und k≡4, 24 (mod 30) |
| 15 | v≡0 (mod 12) und k≡4, 7 (mod 12) ; v≡3 (mod 12) und k≡7 (mod 12);<br>v≡8 (mod 12) und k≡0, 3, 4, 7 (mod 12) ; v≡11 (mod 12) und k≡3, 7 (mod 12);<br>**mit Ausnahme der Werte (k,v) für die $\mu_2(5, k, v)=3$** |
| 20 | v≡1 (mod 6) und k≡0 (mod 2) ; v≡3 (mod 6) und k≡0, 2 (mod 6) ;<br>v≡5 (mod 6) und k≡2 (mod 6)<br>**mit Ausnahme der Werte (k,v) für die $\mu_2(5, k, v)=4$** |
| 30 | v≡0 (mod 12) und k≡1, 10 (mod 12) ; v≡2 (mod 12) und k≡0, 1 (mod 3) ;<br>v≡3 (mod 12) und k≡1 (mod 12) ; v≡5 (mod 12) und k≡1, 3 (mod 6) ;<br>v≡6 (mod 12) und k≡1 (mod 3) ; v≡8 (mod 12) und k≡1, 6, 9, 10 (mod 12) ;<br>v≡9 (mod 12) und k≡1, 7 (mod 12) ; v≡10 (mod 12) und k≡1, 9 (mod 12) ;<br>**mit Ausnahme der Werte (k,v) für die $\mu_2(5, k, v)=6$** |
| 60 | v≡3 (mod 6) und k≡4 (mod 6) ; v≡5 (mod 6) und k≡0, 4 (mod 6)<br>**mit Ausnahme der Werte (k,v) für die $\mu_2(5, k, v)=12$** |

$\mu_5(5, k, v)=\mu_4(5, k, v)=\mu_3(5, k, v)=\mu_2(5, k, v)$

# Anhang B Einige bekannte PA und offene Probleme

In den folgenden Tabellen werden die Sätze, Bemerkungen bzw. Beispiele, aus denen sich die aufgelisteten PA ergeben, durch ihre Nummer gekennzeichnet. Werden bekannte kombinatorische Strukturen (meist Designs) verwendet, so sind diese mit einem Literaturverweis versehen. Die mit dem Computer gefundenen PA werden im nächsten Anhang explizit aufgelistet.

## PA mit k=v

### Fall t=2

*a) Optimale PA*

| | |
|---|---|
| $PA_1(2,q,q)$ | q ungerade Primzahlpotenz (3.12) |
| $PA_2(2,q,q)$ | $q=2^f$ (3.3 a) |
| $PA_2(2,6,6)$ | gefunden in [8] Konstruktion siehe auch (3.19) und (3.27) |
| $PA_2(2,10,10)$ | erstmals gefunden vom S.Black mittels simulated Anealing. Konstruktion siehe auch Abschnitt 3.2 |
| $PA_2(2,12,12)$ | Konstruktion (3.27) |

*b) kleines $\lambda$*

| | |
|---|---|
| $PA_{(q-1)/2}(2,q+1,q+1)$ | $q\equiv 1 \pmod 4$ Primzahlpotenz (3.18) |
| $PA_{q-1}(2,q+1,q+1)$ | $q=2^f$ Bemerkung (3.18) bzw, $q\equiv 3 \pmod 4$ PSL(2,q) (3.1) |
| $PA_\lambda(2,q^3+1,q^3+1)$ mit $\lambda=\frac{2(q^2+1)}{ggt(3,q+1)}$ | q>2 Primzahlpotenz (3.3 d) $PSU_3(q)$ |
| $PA_{2(q-1)}(2,q^3+1,q^3+1)$ | $q=3^{ungerade}$ (3.3 e) R(q) |
| $PA_{2(q-1)}(2,q^2+1,q^2+1)$ | $q=2^{ungerade}$ (3.3 f) Sz(q) |
| $PA_{(q-1)}(2,q^2+1,q^2+1)$ | Vermutung für q=3,5,7,9 mit Computer gefunden (∗) |
| $PA_{l(v-1)}(2,v+1,v+1)$ | Aufblasen eines $PA_l(2,v,v)$ siehe (2.33 c) |
| $PA_6(2,14,14)$ | (3.18) für q=13 |
| $PA_{24}(2,15,15)$ | $A_7$ auf 15 Punkten nach (3.1) |
| $PA_8(2,18,18)$ | (3.18) für q=17 |
| $PA_{18}(2,20,20)$ | (2.33 c) für q=19 |
| $PA_{96}(2,21,21)$ | PSL(3,4) nach (3.1) |
| $PA_{22}(2,24,24)$ | (2.33 c) für q=23 |
| $PA_4(2,26,26)$ | (∗) für q=5 |
| $PA_4(2,28,28)$ | (3.3 e) für q=3 |
| $PA_{14}(2,30,30)$ | (3.18) für q=29 |
| $PA_{31}(2,33,33)$ | (3.18) für q=32 |
| $PA_{2304}(2,36,36)$ | Die Gruppe $Sp_6(2)$ ist 2-fach transitiv auf 36 Punkten (3.1) |
| $PA_{18}(2,38,38)$ | (3.18) für q=37 |
| $PA_{20}(2,42,42)$ | (3.18) für q=41 |
| $PA_6(2,50,50)$ | (∗) für q=7 |
| $PA_{14}(2,65,65)$ | (3.3 f) für q=8 |
| $PA_8(2,82,82)$ | (∗) für q=9 |
| $PA_{16}(2,126,126)$ | (3.3 d) für q=5 |
| $PA_{62}(2,1025,1025)$ | (3.3 f) für q=32 |

| | |
|---|---|
| $PA_{52}(2,19684,19684)$ | (3.3 e) für q=27 |

**Fall t=3**

*a) Optimale PA*

| | |
|---|---|
| $PA_3(3,q+1,q+1)$ | q≡3,11(mod 12) (3.3 c) |
| PA(3,v,v) | für v≤5 äquivalent zu optimalen PA(2,v,v) () |
| $PA_3(3,6,6)$ | [15] oder (2.37) |
| $PA_3(3,7,7)$ | Computer; vergleiche (3.26) |
| $PA_1(3,8,8)$ | (3.4) AGL(2,7) |
| $PA_3(3,9,9)$ | [8] |
| $PA_3(3,12,12)$ | (3.3 c) für q=11 |
| $PA_3(3,24,24)$ | (3.3 c) für q=23 |
| $PA_3(3,28,28)$ | (3.3 c) für q=27 |
| $PA_1(3,32,32)$ | (3.4) $A\Gamma L_1(32)$ |
| $PA_3(3,48,48)$ | (3.3 c) für q=47 |

*b) kleines $\lambda$*

| | |
|---|---|
| $PA_3(3,q+1,q+1)$ | q≡3(mod4) Primzahlpotenz (3.3 c) PSL(2,q) |
| $PA_6(3,q+1,q+1)$ | q Primzahlpotenz (3.3 b) PGL(2,q) |
| $PA_6(3,10,10)$ | (3.3 b) für q=9 |
| $PA_4(3,11,11)$ | Computer siehe Anhang C |
| $PA_{30}(3,13,13)$ | (2.33 c) mit $PA_3(3,12,12)$ |
| $PA_6(3,14,14)$ | (3.3 c) für q=13 |
| $PA_{72}(3,15,15)$ | (2.33 c) mit $PA_6(3,14,14)$ |
| $PA_{72}(3,16,16)$ | $E_{16}\cdot A_7$ |
| $PA_6(3,17,17)$ | (3.3 b) für q=16 |
| $PA_3(3,18,18)$ | (3.3 c) für q=17 |
| $PA_{48}(3,19,19)$ | (2.33 c) mit $PA_3(3,18,18)$ |
| $PA_3(3,20,20)$ | (3.3 c) für q=19 |
| $PA_{54}(3,21,21)$ | (2.33 c) mit $PA_3(3,20,20)$ |

**Fall t=4**

*a) Optimale PA*

| | |
|---|---|
| PA(4,v,v) | für v≤7 äquivalent zu optimalen PA(3,v,v) (2.13 b) |
| $PA_4(4,8,8)$ | Computer |

*b) kleines $\lambda$*

| | |
|---|---|
| $PA_4(4,9,9)$ | (3.4) PGL(2,8) |
| $PA_{24}(4,10,10)$ | (2.33 c) mit $PA_4(4,9,9)$ |
| $PA_{24}(4,11,11)$ | (3.4) $M_{11}$ |
| $PA_{192}(4,12,12)$ | (3.4) $M_{12}$ oder (3.33 c) mit $PA_{24}(4,11,11)$ |
| $PA_4(4,33,33)$ | (3.4) $P\Gamma L_2(32)$ |

**Fall t>4**

*kleines $\lambda$*

| | |
|---|---|
| PA(t,v,v) | für $\lfloor v/2 \rfloor \leq t$ ist äquivalent einem PA($\lfloor v/2 \rfloor$,v,v) (2.13 b) |

| | |
|---|---|
| $PA_{20}(5,10,10)$ | (2.33 c) mit $PA_4(5,9,9)$ |
| $PA_{120}(5,12,12)$ | $M_{12}$ siehe (3.4) |
| $PA_{360}(6,12,12)$ | $PA_6(6,9,9)$ und vollständiger Design 6-(12,9,20) und $PA_3(3,3,3)$ (2.30) |
| $PA_{2520}(6,13,13)$ | $PA_6(6,9,9)$ und vollständiger Design 6-(13,9,35) und $PA_{12}(4,4,4)$ (2.30) |
| $PA_{2940}(8,14,14)$ | $PA_{14}(8,9,9)$ und vollständiger Design 7-(14,9,21) und $PA_{10}(5,5,5)$ (2.30) |

## s-PA(t,k,v) mit k<v

Steht in der Spalte der optimalen PA der Ausdruck, s..s'-$PA_\lambda$(t,{k,..,k'},v), so soll dies gelesen werden als: Es gibt ein s'-$PA_\lambda$(t,l,v) für alle l∈ {k,..,k'}. Diese sind auch optimal als u-PA für alle u= s..s'.

0-PA erhält man als Restriktion aus allen PA aus Teil 1 (2.11 i)

**Fall t=2**

*a) Optimale PA*

| | |
|---|---|
| 1-$PA_1(2,k,q)$ | k,q ungerade, q Primzahlpotenz k\|q oder k\|(q-1) (3.15) |
| 1-$PA_2(2,k,q)$ | k gerade oder $q=2^f$ q= Primzahlpotenz (3.3 a) |
| 1-$PA_2(2,2,v)$ | alle v≥2(2.26) |
| 1-$PA_1(2,3,v)$ | alle v≥3 [20] |
| 1-$PA_2(2,4,v)$ | alle v≥4, Da 3 MOLS für alle außer v=6 oder v=10 bekannt, folgt mit (1.11 a) und (3.2) die Existenz der 1-PA für alle v außer v=6 oder v=10. Diese siehe Anhang C. |
| 1-$PA_1(2,5,v)$ | v≡1,5(mod10) außer v=15 [19]. |
| 1-PA(2,k,$q^n$) | q prim mit 1-PA(2,k,q) und 2-($q^n$,q,1)[1], für alle k für die ein optimales 1-PA(2,k,q) existiert. (2.23 b) |
| 1-PA(2,k,$q^n$+..+q+1) | q prim mit 1-PA(2,k,q+1) und 2-($q^n$+..+q+1,q+1,1)[1], für alle k für die ein optimales 1-PA(2,k,q+1) existiert (für ungerades n falls k und q ungerade). (2.23) |
| 1-PA(2,k,$q^3$+1) | q prim mit 1-PA(2,k,q+1) und 2-($q^3$+1,q+1,1)[1], für alle k für die ein optimales 1-PA(2,k,q+1) existiert. (2.23) |
| 1-$PA_2(2,\{3..6\},6)$ | siehe (3.19), für k=4 Computer. |
| 1-$PA_2(2,\{3..5,9\},10)$ | Abschnitt 3.2 und Anhang C |
| 1-$PA_2(2,\{3..6,11\},12)$ | in [9] wird ein $OD_1(2,6,12)$ konstruiert und (3.2) |
| 0-$PA_1(2,5,15)$ | [22] |
| 1-$PA_1(2,\{5,9\},19)$ | (3.15) |
| 1-$PA_1(2,\{5,7,9,11\},23)$ | in AGL(2,23) mit Computer teils auch mit (3.15) |
| 1-$PA_1(2,\{5,7,9,13,15\},27)$ | in AGL(2,27) mit Computer teils auch mit (3.15) |
| 1-$PA_2(2,7,28)$ | $PA_1(2,7,7)$ und 2-(28,7,2) [1] siehe(2.23 b) |
| 1-$PA_1(2,\{5,7,9,11,15\},31)$ | in AGL(2,31) mit Computer teils auch mit (3.15) |
| 1-$PA_1(2,\{5,7,9,11\},43)$ | in AGL(2,43) mit Computer teils auch mit (3.15) |
| 1-$PA_1(2,\{5,7,9,11\},47)$ | in AGL(2,47) mit Computer teils auch mit (3.15) |
| 1-$PA_2(2,\{5,11\},56)$ | $PA_1(2,\{5,11\},11)$ und 2-(56,11,2) [1] siehe (2.23 b) |
| 1-$PA_2(2,\{6,8\},57)$ | 1-$PA_2(2,\{6,8\},8)$ und 2-(57,8,1) [1] siehe(2.23 b) |
| 1-$PA_1(2,\{5,7,9,11\},59)$ | in AGL(2,59) mit Computer teils auch mit (3.15) |

| | |
|---|---|
| 1-$PA_1$(2,5,61) | [19] |
| 1-$PA_2$(2,6,61) | $PA_2$(2,6,6) und 2-(61,6,1) [1] siehe(2.23 b) |
| 1-$PA_2$(2,6,66) | $PA_2$(2,6,6) und 2-(66,6,1) [1] siehe(2.23 b) |
| 1-$PA_2$(2,11,66) | $PA_1$(2,11,11) und 2-(66,11,2) [1] siehe(2.23 b) |
| 1-$PA_1$(2,{5,7,9,11,13},67) | in AGL(2,67) mit Computer teils auch mit (3.15) |
| 1-$PA_1$(2,{5,7,9,11,13},71) | in AGL(2,71) mit Computer teils auch mit (3.15) |
| 1-$PA_1$(2,9,73) | 1-$PA_1$(2,9,9) und 2-(73,9,1) [1] siehe(2.23 b) |
| 1-$PA_2$(2,6,76) | $PA_2$(2,6,6) und 2-(76,6,1) [1] siehe(2.23 b) |
| 1-$PA_1$(2,{5,7,9,11,13},79) | in AGL(2,79) mit Computer teils auch mit (3.15) |
| 1-$PA_1$(2,{5,7,9,11,13},83) | in AGL(2,83) mit Computer teils auch mit (3.15) |
| 1-$PA_1$(2,7,91) | $PA_1$(2,7,7) und 2-(91,7,1) [1] siehe(2.23 b) |
| 1-$PA_2$(2,10,91) | [19] |
| 1-$PA_1$(2,{5,7,9,11,13,15}, 103) | in AGL(2,103) mit Computer teils auch mit (3.15) |

*b) kleines $\lambda$*

| | |
|---|---|
| 1-$PA_2$(2,k,q) | (k, q ungerade, q Primzahlpotenz) (3.3 a) |
| $PA_{(q-1)/2}$(2,k,q+1) | q≡1(mod4) Primzahlpotenz k/((q+1)/2) oder k/q ungerade (3.19) |
| $PA_{q-1}$(2,k,q+1) | k≥2 ungerade, q Primzahlpotenz PSL(2,q) (3.2) |
| $PA_{q-1}$(2,k,q+1) | $q=2^f$ k/(q+1) oder k/(q-1) ungerade (3.19) |
| $PA_\lambda$(2,k,$q^3$+1) mit $\lambda = \frac{2(q^2+1)}{ggt(3,q+1)}$ | q>2 Primzahlpotenz (3.3 d) $PSU_3$(q) |
| $PA_{2(q-1)}$(2,k,$q^3$+1) | $q=3^{ungerade}$ (3.3 e) R(q) |
| $PA_{2(q-1)}$(2,k,$q^2$+1) | $q=2^{ungerade}$ (3.3 f) Sz(q) |
| $PA_{(q-1)}$(2,k,$q^2$+1) | q=5,7,9 und k/(($q^2$+1)/2) oder k/$q^2$ Computer (∗) |
| 1-$PA_\lambda$(2,k,$q^n$) | q Prim mit 1-$PA_\lambda$(2,k,q) und 2-($q^n$,q+1,1) [1] für alle k für die ein 1-$PA_\lambda$(2,k,q) existiert. (2.23 b) |
| 1-$PA_\lambda$(2,k,$q^n$+..+q+1) | q Prim mit 1-$PA_\lambda$(2,k,q+1) und 2-($q^n$+..+q+1,q+1,1) [1] für alle k für die ein 1-$PA_\lambda$(2,k,q+1) existiert. (2.23 b) |
| 1-$PA_\lambda$(2,k,$q^3$+1) | q Prim mit 1-$PA_\lambda$(2,k,q+1) und 2-($q^3$+1,q+1,1) [1] für alle k für die ein 1-$PA_\lambda$(2,k,q+1) existiert. (2.23 b) |
| 1-$PA_6$(2,{7,13},14) | (3.19) für q=13 |
| 1-$PA_3$(2,7,15) | $PA_1$(2,7,7) und 2-(15,7,3) [1] siehe(2.23 b) |
| 1-$PA_6$(2,{7,13},18) | (3.19) für q=17 |
| 1-$PA_3$(2,5,21) | $PA_1$(2,7,7) und 2-(21,5,3) [1] siehe(2.23 b) |
| 1-$PA_3$(2,7,21) | $PA_1$(2,7,7) und 2-(21,7,3) [1] siehe(2.23 b) |
| 1-$PA_4$(2,7,22) | $PA_1$(2,7,7) und 2-(22,7,4) [1] siehe(2.23 b) |
| 1-$PA_4$(2,{5,13,25},26) | (∗) q=5 |
| 1-$PA_4$(2,k,28) | k≥2 (3.3 e) für q=3 |
| 1-$PA_3$(2,9,33) | $PA_1$(2,9,9) und 2-(33,9,3) [1] siehe(2.23 b) |
| 1-$PA_4$(2,6,36) | $PA_2$(2,6,6) und 2-(36,6,2) [1] siehe(2.23 b) |
| 1-$PA_4$(2,13,40) | $PA_1$(2,13,13) und 2-(40,13,4) [1] siehe(2.23 b) |
| 1-$PA_2$(2,9,45) | $PA_1$(2,9,9) und 2-(45,9,2) [1] siehe(2.23 b) |
| 1-$PA_6$(2,{5,7,25,49},50) | (∗) q=7 |
| 1-$PA_8$(2,{3,4,27,41,81},82) | (∗) q=9 |

**Fall t=3**

*a) Optimale PA*

| | |
|---|---|
| 1..3-$PA_3(3,k,q+1)$ | q Primzahlpotenz. $q \not\equiv 1,4 \pmod 6$ oder $k \not\equiv 2,5 \pmod 6$ (3.3 c) |
| 1..3-$PA_6(3,k,q+1)$ | q Primzahlpotenz. k, q gerade außer $q \equiv 4 \pmod 6$ und $k \equiv 2 \pmod 6$ (3.3 c) |
| 1..3-$PA_3(3,3,v)$ | siehe (2.26) |
| 1..3-$PA(3,4,v)$ | außer v=7 siehe (2.24 2) |
| 1..3-$PA_3(3,5,6)$ | siehe (2.25) |
| 1..3-$PA_3(3,5,9^n+1)$ | $PA_1(3,5,5)$ und 3-(10,5,3) [12] 3-($9^n$+1,10,1) [1] siehe(2.23 b) |
| 1..3-$PA_3(3,8,16)$ | $PA_1(3,8,8)$ und 3-(16,8,3) [12] siehe(2.23 b) |
| 1..3-$PA_1(3,5,4^n+1)$ | $PA_1(3,5,5)$ und 3-($4^n$+1,5,1) [1] siehe(2.23 b) |
| 1..3-$PA_3(3,5,21)$ | $PA_1(3,5,5)$ und 3-(21,5,3) [12] siehe(2.23 b) |
| 1..3-$PA_3(3,5,22)$ | $PA_1(3,5,5)$ und 3-(22,5,3) [12] siehe(2.23 b) |
| 1..3-$PA_3(3,6,22)$ | $PA_3(3,6,6)$ und 3-(22,6,1) [12] siehe(2.23 b) |
| 1..3-$PA_3(3,5,25)$ | $PA_1(3,5,5)$ und 3-(25,5,3) [12] siehe(2.23 b) |
| 1..3-$PA_1(3,5,25^n+1)$ | $PA_1(3,5,5)$ und 3-(26,5,1) [12] und 3-($25^n$+1,26,1) [1] siehe(2.23 b) |
| 1..3-$PA_3(3,6,5^n+1)$ | $PA_3(3,6,6)$ und 3-($5^n$+1,6,1) [1] siehe(2.23 b) |
| 1..3-$PA_3(3,5,30)$ | $PA_1(3,5,5)$ und 3-(30,5,3) [12] siehe(2.23 b) |
| 1..3-$PA_1(3,8,7^n+1)$ | 3-$PA_1(3,8,8)$ und 3-($7^n$+1,8,1) [1] siehe(2.23 b) |

*b) kleines $\lambda$*

| | |
|---|---|
| 3-$PA_3(3,k,q+1)$ | $q \equiv 3 \pmod 4$ Primzahlpotenz (3.3 c)( falls nicht optimal) |
| 3-$PA_6(3,k,q+1)$ | q Primzahlpotenz (3.3 c) ( falls nicht optimal) |
| 3-$PA_4(3,5,11)$ | $PA_1(3,5,5)$ und 3-(11,5,4) [12] siehe(2.23 b) |
| 3-$PA_{15}(3,5,13)$ | $PA_1(3,5,5)$ und 3-(13,5,15) [12] siehe(2.23 b) |
| 3-$PA_5(3,5,14)$ | $PA_1(3,5,5)$ und 3-(14,5,5) [12] siehe(2.23 b) |
| 3-$PA_6(3,5,15)$ | $PA_1(3,5,5)$ und 3-(15,5,6) [12] siehe(2.23 b) |
| 3-$PA_6(3,5,16)$ | $PA_1(3,5,5)$ und 3-(16,5,6) [12] siehe(2.23 b) |
| 3-$PA_{18}(3,6,16)$ | $PA_3(3,6,6)$ und 3-(16,6,6) [12] siehe(2.23 b) |
| 3-$PA_{12}(3,6,16^n+1)$ | $PA_1(3,5,17)$ nach (2.33b) und 3-($16^n$+1,17,1) [1] siehe(2.23 b) |
| 3-$PA_{12}(3,7,22)$ | $PA_3(3,7,7)$ und 3-(22,7,4) [12] siehe(2.23 b) |
| 3-$PA_{12}(3,8,22)$ | $PA_1(3,8,8)$ und 3-(22,8,12) [12] siehe(2.23 b) |
| 3-$PA_{10}(3,5,23)$ | $PA_1(3,5,5)$ und 3-(23,5,10) [12] siehe(2.23 b) |
| 3-$PA_{15}(3,7,23)$ | $PA_3(3,7,7)$ und 3-(23,7,5) [12] siehe(2.23 b) |
| 3-$PA_{16}(3,8,23)$ | $PA_1(3,8,8)$ und 3-(23,8,16) [12] siehe(2.23 b) |
| 3-$PA_6(3,5,27)$ | $PA_1(3,5,5)$ und 3-(27,5,6) [12] siehe(2.23 b) |
| 3-$PA_{12}(3,6,27)$ | $PA_3(3,6,6)$ und 3-(27,6,4) [12] siehe(2.23 b) |
| 3-$PA_5(3,5,29)$ | $PA_1(3,5,5)$ und 3-(29,5,5) [12] siehe(2.23 b) |
| 3-$PA_8(3,8,29)$ | $PA_1(3,8,8)$ und 3-(29,8,8) [12] siehe(2.23 b) |
| 3-$PA_6(3,5,31)$ | $PA_1(3,5,5)$ und 3-(31,5,6) [12] siehe(2.23 b) |
| 3-$PA_2(3,5,32)$ | $PA_1(3,5,5)$ und 3-(32,5,2) [12] siehe(2.23 b) |

**Fall t=4**

*a) Optimale PA*

| | |
|---|---|
| 2..4-$PA_{12}$(4,4,v) | siehe (2.26) |
| 1..4-$PA_{12}$(4,4,5) | siehe (2.25) |
| 1..4-$PA_{4}$(4,5,6) | siehe (2.25) |
| 1..4-$PA_{12}$(4,4,7) | siehe (2.25) |
| 1..4-$PA_{6}$(4,5,7) | siehe (2.25) |
| 1..4-$PA_{12}$(4,6,7) | siehe (2.25) |
| 1..4-$PA_{12}$(4,7,8) | siehe (2.25) |
| 0-$PA_{2}$(4,5,9) | siehe Anhang C |
| 0-$PA_{12}$(4,6,10) | 0-$PA_{2}$(4,5,9) siehe(2.33 c) |
| 1..4-$PA_{2}$(4,5,11) | $PA_{2}$(4,5,5) und 4-(11,5,1) [1] siehe(2.23 b) |
| 1..4-$PA_{12}$(4,6,11) | $PA_{2}$(4,5,5) und 4-(11,5,1) [1] siehe (2.33 a) |
| 1..4-$PA_{2}$(4,5,23) | $PA_{2}$(4,5,5) und 4-(23,5,1) [1] siehe(2.23 b) |
| 1..4-$PA_{3}$(4,7,23) | $PA_{3}$(4,7,7) und 4-(23,7,1) [1] siehe(2.23 b) |
| 1..4-$PA_{4}$(4,6,27) | $PA_{4}$(4,6,6) und 4-(27,6,1) [1] siehe(2.23 b) |
| 1..4-$PA_{2}$(4,5,47) | $PA_{2}$(4,5,5) und 4-(47,5,1) [1] siehe(2.23 b) |
| 1..4-$PA_{2}$(4,5,71) | $PA_{2}$(4,5,5) und 4-(71,5,1) [1] siehe(2.23 b) |
| 1..4-$PA_{2}$(4,5,83) | $PA_{2}$(4,5,5) und 4-(83,5,1) [1] siehe(2.23 b) |

*b) kleines $\lambda$*

| | |
|---|---|
| 4-$PA_{24}$(4,k,11) | $M_{11}$ (3.2) |
| 4-$PA_{16}$(4,5,12) | $PA_{2}$(4,5,11) und vollst Design 4-(12,11,8) siehe(2.23 a) |
| 4-$PA_{16}$(4,6,12) | $PA_{2}$(4,5,11) siehe(2.33 c) |
| 4-$PA_{36}$(4,6,23) | 1..4-$PA_{2}$(4,5,23) siehe(2.33 d) |
| 4-$PA_{48}$(4,8,23) | 1..4-$PA_{3}$(4,7,23) siehe(2.33 d) |
| 4-$PA_{360}$(4,9,23) | 1..4-$PA_{3}$(4,7,23) siehe(2.33 d) |
| 4-$PA_{1152}$(4,k,23) | $M_{11}$ (3.2) |
| 4-$PA_{40}$(4,5,24) | $PA_{2}$(4,5,23) und vollst Design 4-(24,23,20) siehe(2.23 a) |
| 4-$PA_{40}$(4,6,24) | $PA_{2}$(4,5,23) siehe(2.33 c) |
| 4-$PA_{84}$(4,7,27) | 1..4-$PA_{4}$(4,6,27) siehe(2.33 d) |
| 4-$PA_{96}$(4,7,28) | 1..4-$PA_{4}$(4,6,27) siehe(2.33 c) |

**Fall t=5**

*a) Optimale PA*

| | |
|---|---|
| 2..5-$PA_{10}$(5,5,v) | siehe (2.26) |
| 1..5-$PA_{10}$(5,5,6) | siehe (2.25) |
| 1..5-$PA_{10}$(5,5,7) | siehe (2.25) |
| 1..5-$PA_{20}$(5,6,7) | siehe (2.25) |
| 2..5-$PA_{10}$(5,5,8) | siehe (2.25) |
| 2..5-$PA_{30}$(5,6,8) | siehe (2.25) |
| 1..5-$PA_{15}$(5,7,8) | siehe (2.25) |
| 2..5-$PA_{30}$(5,7,9) | siehe (2.25) |
| 1..5-$PA_{20}$(5,8,9) | siehe (2.25) |
| 0-$PA_{2}$(5,5,9) | siehe Anhang C |
| 0-$PA_{10}$(5,6,10) | 0-$PA_{2}$(5,5,9) siehe(2.33 c) |

| | |
|---|---|
| 2..5-$PA_{10}$(5,6,12) | $PA_{10}$(5,6,6) und 5-(12,6,1) [1] siehe(2.23 b) |
| 2..5-$PA_{10}$(5,6,24) | $PA_{10}$(5,6,6) und 5-(24,6,1) [1] siehe(2.23 b) |
| 1..5-$PA_5$(5,8,24) | $PA_5$(5,8,8) und 5-(24,8,1) [1] siehe(2.23 b) |
| 1..5-$PA_5$(5,7,28) | $PA_5$(5,7,7) und 5-(28,7,1) [1] siehe(2.23 b) |
| 2..5-$PA_{10}$(5,6,48) | $PA_{10}$(5,6,6) und 5-(48,6,1) [1] siehe(2.23 b) |
| 2..5-$PA_{10}$(5,6,72) | $PA_{10}$(5,6,6) und 5-(72,6,1) [1] siehe(2.23 b) |
| 2..5-$PA_{10}$(5,6,84) | $PA_{10}$(5,6,6) und 5-(84,6,1) [1] siehe(2.23 b) |

*b) kleines $\lambda$*

| | |
|---|---|
| 5-$PA_{10}$(5,9,10) | siehe (2.25) |
| 5-$PA_{60}$(5,7,12) | 5-$PA_{10}$(5,6,12) siehe(2.33 d) |
| 5-$PA_{120}$(5,k,12) | $M_{12}$ (3.2) |
| 5-$PA_{60}$(5,6,13) | 5-$PA_{10}$(5,6,12) vollst Design 4-(13,12,6) siehe(2.23 b) |
| 5-$PA_{60}$(5,7,13) | 5-$PA_{10}$(5,6,12) siehe(2.33 c) |
| 5-$PA_{80}$(5,9,24) | 5-$PA_5$(5,8,24) siehe(2.33 d) |
| 5-$PA_{600}$(5,10,24) | 5-$PA_5$(5,8,24) siehe(2.33 d) |
| 5-$PA_{2800}$(5,11,24) | 5-$PA_5$(5,8,24) siehe(2.33 d) |
| 5-$PA_{5760}$(5,k,24) | $M_{24}$ (3.2) |
| 5-$PA_{100}$(5,8,25) | 5-$PA_5$(5,8,24) vollst Design 4-(25,24,20) siehe(2.23 b) |
| 5-$PA_{80}$(5,9,25) | 5-$PA_5$(5,8,24) siehe(2.33 c) |

**Fall t=6**

*a) Optimale PA*

| | |
|---|---|
| 3..6-$PA_{60}$(6,6,v) | siehe (2.26) |
| 1..6-$PA_{60}$(6,6,7) | siehe (2.25) |
| 2..6-$PA_{60}$(6,6,8) | siehe (2.25) |
| 1..6-$PA_{30}$(6,7,8) | siehe (2.25) |
| 2..6-$PA_{45}$(6,7,9) | siehe (2.25) |
| 1..6-$PA_{30}$(6,8,9) | siehe (2.25) |
| 2..6-$PA_{60}$(6,7,10) | siehe (2.25) |
| 2..6-$PA_{60}$(6,8,10) | siehe (2.25) |

*b) doppelt so groß als optimal*

| | |
|---|---|
| 1..6-$PA_{24}$(6,9,10) | siehe (2.25) |
| 1..6-$PA_{60}$(6,9,11) | siehe (2.25) |
| 1..6-$PA_{120}$(6,10,11) | siehe (2.25) |
| 2..6-$PA_{120}$(6,9,12) | $PA_6$(6,9,9) und vollständiger Design 6-(12,9,20) (2.23 b) |
| 2..6-$PA_{360}$(6,10,12) | $PA_6$(6,9,9) und vollständiger Design 6-(12,9,20) (2.33 a) |

*c) kleines $\lambda$*

| | |
|---|---|
| 6-$PA_{360}$(6,11,12) | $PA_6$(6,9,9) und vollständiger Design 6-(12,9,20) und $PA_1$(2,2,3) (2.30) |
| 6-$PA_{210}$(6,9,13) | $PA_6$(6,9,9) und vollständiger Design 6-(13,9,35) (2.23 b) |
| 6-$PA_{840}$(6,10,13) | $PA_6$(6,9,9) und vollständiger Design 6-(13,9,35) u (2.33 a) |
| 6-$PA_{840}$(6,11,13) | $PA_6$(6,9,9) und vollständiger Design 6-(12,9,20) und $PA_2$(2,2,4) (2.30) |

| | |
|---|---|
| 6-$PA_{840}$(6,12,13) | $PA_6$(6,9,9) und vollständiger Design 6-(12,9,20) und $PA_3$(3,3,4) (2.30) |

**Fall t=7**

*a) Optimale PA*

| | |
|---|---|
| 3..7-$PA_{105}$(7,7,v) | siehe (2.26) |
| 1..7-$PA_{105}$(7,7,8) | siehe (2.25) |
| 2..7-$PA_{105}$(7,7,9) | siehe (2.25) |
| 1..7-$PA_{70}$(7,8,9) | siehe (2.25) |
| 2..7-$PA_{105}$(7,7,10) | siehe (2.25) |
| 2..7-$PA_{105}$(7,8,10) | siehe (2.25) |
| 3..7-$PA_{140}$(7,8,11) | siehe (2.25) |

*b) doppelt so groß als optimal*

| | |
|---|---|
| 1..7-$PA_{42}$(7,9,10) | siehe (2.25) |
| 1..7-$PA_{84}$(7,9,11) | siehe (2.25) |
| 2..7-$PA_{140}$(7,9,12) | siehe (2.25) |
| 1..7-$PA_{168}$(7,10,11) | siehe (2.25) |
| 2..7-$PA_{420}$(7,10,12) | siehe (2.25) |
| 1..7-$PA_{210}$(7,9,13) | $PA_{14}$(7,9,9) und vollständiger Design 7-(13,9,15) (2.23 b) |

*c) kleines $\lambda$*

| | |
|---|---|
| 7-$PA_{840}$(7,10,13) | $PA_6$(6,9,9) und vollständiger Design 6-(13,9,35) (2.33 a) |
| 7-$PA_{5880}$(7,{11..12},13) | $PA_6$(6,9,9) und vollständiger Design 6-(13,9,35) und PA(i,i4)(2.30) |
| 7-$PA_{294}$(7,9,14) | $PA_{14}$(7,9,9) und vollständiger Design 7-(14,9,21) (2.23 b) |
| 7-$PA_{1570}$(7,10,14) | $PA_{14}$(7,9,9) und vollständiger Design 6-(14,9,21) (2.33 a) |
| 7-$PA_{2940}$(7,{11..13},14) | $PA_{14}$(7,9,9) und vollständiger Design 6-(14,9,21) und PA(i,i,5) (2.30) |

**Fall t=8**

*a) Optimale PA*

| | |
|---|---|
| 4..8-$PA_{280}$(8,8,v) | siehe (2.26) |
| 1..8-$PA_{280}$(8,8,9) | siehe (2.25) |
| 2..8-$PA_{280}$(8,8,10) | siehe (2.25) |
| 3..8-$PA_{280}$(8,8,11) | siehe (2.25) |

*b) doppelt so groß als optimal*

| | |
|---|---|
| 1..8-$PA_{112}$(8,9,10) | siehe (2.25) |
| 1..8-$PA_{166}$(8,9,11) | siehe (2.25) |
| 2..8-$PA_{224}$(8,9,12) | siehe (2.25) |
| 1..8-$PA_{280}$(8,9,13) | siehe (2.25) |
| 1..8-$PA_{336}$(8,10,11) | siehe (2.25) |

| | |
|---|---|
| 2..8-$PA_{672}$(8,10,12) | siehe (2.25) |
| 3..8-$PA_{1120}$(8,10,13) | siehe (2.25) |
| 2..8-$PA_{336}$(8,9,14) | $PA_{56}$(8,9,9) und vollständiger Design 8-(14,9,6) (2.23 b) |
| 2..8-$PA_{1860}$(8,10,14) | $PA_{56}$(8,9,9) und vollständiger Design 8-(14,9,6) (2.33 a) |

*c) kleines $\lambda$*

| | |
|---|---|
| 8-$PA_{3360}$(8,{11..13},14) | $PA_{56}$(8,9,9) und vollständiger Design 8-(14,9,6) und PA(i,i,5)(2.30) |
| 8-$PA_{392}$(8,9,15) | $PA_{56}$(8,9,9) und vollständiger Design 8-(15,9,7) (2.23 b) |
| 8-$PA_{2352}$(8,10,15) | $PA_{56}$(8,9,9) und vollständiger Design 8-(15,9,7) (2.33 a) |

**Fall t=9**

*doppelt so groß als optimal*

| | |
|---|---|
| 4..9-$PA_{504}$(9,9,v) | siehe (2.26) |
| 1..9-$PA_{1008}$(9,10,11) | siehe (2.25) |
| 2..9-$PA_{1512}$(9,10,12) | siehe (2.25) |
| 3..9-$PA_{2016}$(9,10,13) | siehe (2.25) |
| 2..9-$PA_{2520}$(9,10,14) | siehe (2.25) |
| 3..9-$PA_{3024}$(9,10,15) | $PA_{504}$(9,9,9) und vollständiger Design 9-(15,9,1) (2.33 a) |

**Fall t=10**

*doppelt so groß als optimal*

| | |
|---|---|
| 5.. 10-$PA_{5040}$(10,10,v) | siehe (2.26) |

## Kleinste offene Probleme

In [6] hat Bierbrauer gezeigt, daß die 1-$PA_1$(2,3,5), 1-$PA_1$(2,5,7), 1-$PA_1$(2,7,9) und 2-$PA_1$(3,5,8) nicht existieren. Damit bleiben als kleinste offene Probleme für den

**Fall k=v**

$PA_2$(2,14,14)
$PA_1$(2,15,15)
$PA_2$(2,18,18)
$PA_3$(3,10,10)
$PA_1$(3,11,11)
$PA_2$(4,9,9)
$PA_{12}$(4,10,10)
$PA_1$(4,11,11)
$PA_{10}$(5,10,10)
$PA_5$(5,11,11)
$PA_{30}$(6,12,12)

**Fall k<v, s=0**

0-$PA_2$(2,5,14)
0-$PA_1$(2,6,15)
0-$PA_3$(3,6,10)
0-$PA_2$(5,6,9)

**Fall k<v, s=1**

1-$PA_1$(2,5,9)
1-$PA_2$(2,{6..8},10)
1-$PA_1$(2,{7,9},11)
1-$PA_1$(2,5,13)
1-$PA_1$(2,5,15)
1-$PA_1$(2,5,17)
1-$PA_6$(3,4,7)
1-$PA_3$(3,5,7)
1-$PA_1$(3,5,8)
1-$PA_4$(4,4,6)
1-$PA_4$(4,5,7)
1-$PA_5$(5,5,8)

**Fall k<v, s=2**

2-$PA_6$(3,4,7)
2-$PA_3$3,5,7)
(2-$PA_{30}$(6,6,9))

**Fall k<v, s=3**

3-$PA_3$(4,5,7)
(3-$PA_{56}$(8,8,12))

# Anhang C Explizite Angabe der s-PA, die mit dem Computer gefunden wurden

## 1. 0-PA(t, k, v)

**$PA_2$(2, v, v) der Form G$\cup$GσG** (siehe auch Beispiel (3.xx)).

Existiert für v=6 mit:

$G =< (0,1,2,3,4) >$.

σ= 0 ∞ 1 3 2 4

für v=12 mit:

$G =< () >$.

σ= 0 ∞ 7 5 1 6 2 4 1 9 8 3

0

Keine solchen PA existieren für:

$v \in \{10,14,18,20\}$

**$PA_{q-1}$(2, $q^2$+1, $q^2$+1) der Form LVR in P$\Gamma L_2(q^2+1)$**

Diese existieren für $q \in \{3,5,7,9\}$. dabei ist L eine elementarabelsche Gruppe der Ordnung $q^2$ und R eine zyklische Gruppe der Ordnung $\frac{q^2+1}{2}$

Fall q=3:

V:

1 2 3 4 5 6 7 8 9 10
1 4 9 6 8 2 5 10 7 3

Erzeugende von L:

2 3 1 5 6 4 8 9 7 10
4 5 6 7 8 9 1 2 3 10

Erzeugende von R:

5 4 8 9 6 7 10 2 3 1

Fall q=5
V:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
1 2 20 15 16 19 21 17 14 11 25 3 5 22 18 13 23 4 24 12 26 9 8 6 10 7
1 2 7 20 15 17 5 10 6 22 14 21 18 24 3 4 25 12 8 26 13 19 11 23 9 16
1 2 15 16 7 9 3 19 25 8 23 18 21 11 5 26 6 13 22 4 12 10 24 14 17 20

Erzeugende von L:

2 3 4 5 1 7 8 9 10 6 12 13 14 15 11 17 18 19 20 16 22 23 24 25 21 26
6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 1 2 3 4 5 26

Erzeugende von R:

13 11 10 20 8 7 23 6 17 18 25 14 15 21 9 19 24 12 22 16 26 2 4 3 5 1

Fall q=7

V:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

1 2 46 26 39 22 47 33 24 30 19 3 7 21 25 32 31 23 38 5 40 49 34 20 29 44 36 42 41 4 18 15 6 37 43 17 27 45 35 48 28 16 50 12 14 10 8 11 13 9

1 2 13 33 30 20 43 9 3 47 31 49 35 37 45 19 25 41 18 10 27 5 28 46 14 6 32 48 21 8 29 38 24 42 26 15 16 23 4 36 40 11 44 22 34 7 50 17 39 12

1 2 39 9 47 46 26 30 6 20 28 35 44 15 27 17 38 11 41 8 32 3 48 33 37 50 14 18 34 24 19 36 10 40 13 45 21 29 7 16 23 31 49 43 25 5 4 42 12 22

1 2 24 35 49 44 10 3 47 50 25 20 30 42 23 37 48 21 15 13 28 26 14 7 18 39 19 36 31 43 40 34 12 45 6 11 38 32 22 41 17 27 33 5 16 9 46 29 4 8

1 3 47 13 41 38 19 5 37 50 49 32 10 27 45 24 39 34 29 18 48 44 20 6 35 28 30 22 12 36 23 11 16 40 4 21 26 14 43 25 33 46 9 2 31 17 42 8 7 15

Erzeugende von L:

2 3 4 5 6 7 1 9 10 11 12 13 14 8 16 17 18 19 20 21 15 23 24 25 26 27 28 22 30 31 32 33 34 35 29 37 38 39 40 41 42 36 44 45 46 47 48 49 43 50

8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 1 2 3 4 5 6 7 50

Erzeugende von R:

17 15 32 23 46 24 30 9 27 8 37 20 19 40 25 11 13 22 48 16 44 33 14 42 10 29 45 47 49 18 39 38 21 43 31 41 28 34 12 35 26 36 50 2 5 6 3 4 7 1

Den Fall q=9 lasse ich seines Umfangs halber weg.

**$PA_3(3, 7, 7)$**

Ein $PA_3(3, 7, 7)$ der Form LVR liefert:
L=<(1,2,3,4,5,6,7)>, R=<(3,4,5,6,7)>

$$V = \begin{matrix} 1 & 7 & 2 & 3 & 4 & 6 & 5 \\ 1 & 3 & 2 & 4 & 7 & 6 & 5 \\ 1 & 4 & 2 & 6 & 3 & 5 & 7 \end{matrix}$$

**$PA_4(3, 11, 11)$**

Ein $PA_4(3, 11, 11)$ der Form LVR, der in einer $M_{11}$ liegt, liefert:

L=<2 4 1 6 10 9 5 3 11 8 7> |L|=11

R=<1 4 2 5 7 10 3 11 8 9 6> |R|=/5

V:

1 2 3 6 11 10 4 9 5 7 8
1 2 3 11 7 5 8 6 4 9 10
1 2 8 3 9 6 4 7 11 5 10
1 2 9 6 8 3 11 7 4 10 5
1 2 9 8 10 4 5 6 11 7 3
1 6 4 5 9 2 8 11 7 3 10
1 2 11 8 9 5 6 3 7 10 4
1 7 3 11 9 2 6 4 10 5 8
1 2 11 5 4 10 8 7 9 6 3
1 9 6 5 11 2 10 4 8 7 3

1 2 10 7 11 9 6 8 4 5 3
1 7 9 10 6 2 8 5 4 11 3

**$PA_4(4, 8, 8)$**

Ein $PA_4(4, 8, 8)$ der Form LVR liefert:

L=<(2,3,4,5,6,7,8)>, R=<(4,5,6,7,8)>

V:

1 2 3 4 5 6 7 8
2 1 4 3 5 6 8 7
2 5 1 3 4 6 8 7
2 4 6 1 3 5 8 7
2 6 3 1 4 7 8 5
2 7 8 1 4 6 3 5
2 8 4 1 6 3 5 7
2 8 6 1 4 7 3 5

**$0\text{-}PA_2(5, 5, 9)$**

Ein $0\text{-}PA_2(5, 5, 9)$ der Form LV liefert:

L= <(3,4,5,6,7)>

V:

1 2 3 4 5
1 3 2 4 5
1 3 4 6 2
1 3 5 2 9
3 1 2 6 7
3 1 4 7 2
3 1 6 2 5
3 7 1 9 2
3 5 1 2 7
3 5 8 1 2
3 1 4 5 6
3 4 5 1 6
3 4 5 7 1
3 4 6 1 9
3 4 5 8 1
3 6 9 8 1
3 6 1 7 9
3 8 4 1 7
3 5 7 8 1
3 8 1 6 4
2 3 4 5 6
2 3 4 8 9
3 2 4 9 6
3 6 2 4 9
2 3 8 6 9
3 4 8 2 5
3 2 6 9 5
3 7 2 4 6
2 3 8 6 4
3 2 8 7 5
3 7 4 8 9

3 8 7 9 4
3 9 5 7 4
3 9 7 8 5
3 5 7 4 8
3 7 4 8 5

## 2. 1-PA(t, k, v)

### $APA_2(2, 4, 6)$

Ein $APA_2(2, 4, 6)$ der Form LV wird geliefert durch:

L=<(1,2,3,4,5)>

V:
1 2 3 4
1 2 3 5
1 3 5 6
3 1 6 2
1 6 2 4
6 1 4 5

### $APA_2(2, 4, 10)$

Ein $OD_1(2, 4, 6)$ insbesondere $APA_2(2, 4, 10)$ ein der Form LV wird geliefert durch:

L=<(1,2,3,4,5,5,6,7,8,9)>

2 1 3 4
3 1 2 8
4 1 8 3
5 1 7 6
6 1 9 10
7 1 4 2
8 1 10 5
9 1 5 7
10 1 6 9
1 10 8 4

### $APA_1(2, k, q)$ in der $AG_2(q)$ $q3\equiv(\mathrm{mod}\ 4)$ Primzahlpotenz

Es werden PA gemäß (3.11) konstruiert wobei man $\mathbb{F}_q$ als Ring und die Quadrate in $\mathbb{F}_q^*$ als Halbsystem nimmt. Es ist also eine Spaltenmenge I zu finden die (3.11) und (3.10 d) erfüllt. Die mit (∗) gekennzeichneten Spaltenmengen erfüllen diese Bedingungen auch wenn man sie auf die ersten k (k ungerade) Elemente einschränkt. Es werden hier nur die Parameter (k,q) aufgeführt die sich nicht schon aus (3.15) folgen. Von den hier angegebenen Mengen I muß man von jedem Element 1 abziehen um die gewöhnliche Darstellung der Elemente von $\mathbb{F}_q$ :{0,1,..., q-1) zu erhalten.

q=11, k=3

I: {1, 2, 3}

q=19, k=5

I: {1, 2, 3, 4, 6}

q=23, k=3, 5, 7
I: {1, 2, 6, 3 12 10 16} (∗)
k=9
I: {1, 2, 3, 4, 6, 12, 14, 16, 22}

q=31, k=3,.., 9 (ungerade)
I: {1, 2, 4, 3, 13, 8, 27, 20, 28} (∗)
k=11
I: {1, 2, 3, 4, 5, 7, 9, 13, 17, 18, 25}

q=43, k=3,.., 9 (ungerade)
I: {1, 2, 3, 5, 13, 7, 6, 10, 43} (∗)
k=11
I:, {1, 2, 3, 4, 5, 6, 7, 11, 24, 27, 40}

q=47, k=3,.., 11 (ungerade)
I: {1, 2, 6, 3, 40, 17, 23 15, 44, 8, 21} (∗)

q=59, k=3,..,11 (ungerade)
I: {1, 2, 3, 4, 9, 5, 12, 26, 48, 47, 25} (∗)

q=67, k=3,...,13 (ungerade)
I: {1, 2, 3, 5, 12, 50, 21, 56, 29, 40, 51, 41, 43} (∗)

q=71, k=3,.., 13 (ungerade)
I: {1, 2, 8, 3, 23, 5, 24, 25, 18, 41, 56, 37, 60} (∗)

q=83, k=3,.., 13 (ungerade)
I: {1, 2, 3, 4, 25, 8, 51, 17, 40, 24, 63, 71, 55} (∗)

q=103, k=3,..., 15 (ungerade)
I: {1, 2, 4, 3, 12, 9, 22, 47, 95, 53, 81, 65, 71, 59, 48} (∗)

Für Primzahlpotenzen gebe ich die Körperelemente durch die Polynome in $\mathbb{F}_q[x]$ und das verwendete Primpolynom an. Wobei ich nur die Koeffizienten der Polynome, beginnend mit dem höchsten, angebe.

q=$3^3$, k=5

Primpolynom:
1 1 0 2

I:
0 0 0
0 0 1
0 0 2
0 1 0
1 1 2

k=7
I:
0 0 0
0 0 1
0 0 2
0 1 0
0 1 1
0 2 2
2 1 2

k=15
I:
0 0 0
0 0 1
0 0 2
0 1 0
0 1 1
0 1 2
0 2 0
1 0 0
1 0 2
1 1 1
1 2 2
2 0 2
2 1 1
2 1 2
2 2 2

$q=3^5$, k=5
Primpolynom:
1 1 0 1 0 1
I:
0 0 0 0 0
0 0 0 0 1
0 0 0 0 2
0 0 0 1 0
0 0 2 0 2

$q=3^7$, k=5
Primpolynom:
1 0 0 0 0 1 0 2
I:
0 0 0 0 0 0 0
0 0 0 0 0 0 1
0 0 0 0 0 0 2
0 0 0 0 0 1 0
0 0 0 0 1 0 1

$q=3^{11}$ k=5
Primpolynom:
1 0 0 0 0 0 0 0 0 1 0 2
I:
0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 1
0 0 0 0 0 0 0 0 0 0 0 2
0 0 0 0 0 0 0 0 0 0 1 0
0 0 0 0 0 0 0 0 0 1 0 1

$q=7^3$, k=5
Primpolynom:
1 1 0 1
I:
0 0 0
0 0 1
0 0 2
0 0 3
0 1 1

$q=7^5$, k=5
Primpolynom:
1 0 0 0 1 3
I:
0 0 0 0 0
0 0 0 0 1
0 0 0 0 2
0 0 0 0 3
0 0 0 1 2

$q=7^7$ k=5
Primpolynom:

1 0 0 0 0 0 6 1

I:

0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 1

0 0 0 0 0 0 0 2
0 0 0 0 0 0 0 3
0 0 0 0 2 0 2

## 3. 2-PA(t, k, v)

### 2-$PA_3$(3, 4, 6)

Ein 2-$PA_3$(3, 4, 6) der Form LV liefert:

L=<(1,2,3,4,5)>
V:

1 2 3 4
2 1 3 6
3 2 1 5
1 4 2 5
2 4 1 3
4 1 2 6
1 6 2 3
2 1 6 5
6 2 1 4
1 3 6 5
3 6 1 4
6 3 1 2

# Anhang D Programmbeispiele

Die nachfolgenden PASCAL-Programme sollen illustrieren auf welche Art ich zu den PA, die ich mit dem Computer gefunden habe, gekommen bin. Um die Programme übersichtlich zu halten wurden die Möglichkeiten, um sie zu beschleunigen, nicht ausgenützt. Für die in den Beispielen gesuchten PA reicht die Geschwindigkeit aber völlig aus.

Es liegen den Programmen zwei verschiedene Konzepte zugrunde. Im Programm zu Beispiel (3.26) werden alle für die Suche benötigten Daten vor der Suche erzeugt. Da dieselben Daten um so öfter gebraucht werden je mehr Erzeugende des PA gesucht sind, erzielt man mit dieser Methode dann einen großen Geschwindigkeitsgewinn. Der Nachteil ist der Speicherplatzverbrauch. Reicht der verfügbare Speicherplatz nicht aus so muß man die benötigten Daten für den Test jedesmal neu erzeugen. Falls die Zahl der Erzeugenden klein genug ist, ist dies vertretbar. Das Programm zu Beispiel (3.27) ist von dieser Art.

## Programm zu (3.26)

```
Programm PA;
{  Es wird ein PA_la(3,v,v) gesucht, auf dessen Einträgen eine Gruppe der Ordnung ogl und  }
{  und auf dessen Spalten eine Gruppe der Ordnung ogr operiert.  }

 const
   v = 7;
   la = 3;
   ogr = 5;
   ogl = 7;
   anz = 48;   {  Die Anzahl der Doppelnebenklassen der S7 unter diesen Gruppen  }

   v2 = (v - 1) * v div 2;  {  (v 2)  }
   v3 = (v - 2) * v2 div 3; {  (v 3)  }
   abl = v3 div ogl;  {Anzahl der Bahnen von der Gruppe der Ordnung ogl auf 3-Mengen }
   abr = v3 div ogr;  {Anzahl der Bahnen von der Gruppe der Ordnung ogr auf 3-Mengen}
   az = la * abl div ogr; {Anzahl der Erzeugenden des PA   }

 type
{  Die Datenstrukturen werden bei ihrer Verwendung erläutert.  }
   per = array[1..v] of 1..v;
   apt = array[1..az, 1..anz] of per;
   ter = record
       a: 0..ogr;
       x: 1..abl;
    end;
   tet = array[1..abr, 0..ogr] of ter;
   ttt = array[1..az, 1..anz] of tet;
   grt = array[1..v] of per;
   tut = array[1..v, 1..v, 1..v] of 0..v3;
   ntut = array[1..v3, 1..3] of 1..v;
   bahnlt = array[0..v3] of 0..abl;
   bahnrt = array[0..v3] of 0..abr;
   kont = array[0..abl, 0..abr] of 0..la;
```

```
 var
    i, j, max: integer;
    z: longint;
    gr, gl: grt;
    tu: tut;
    nttu: ntut;
    bahnl: bahnlt;
    bahnr: bahnrt;
    kon: kont;
    a: per;
    ap: ^apt;
    erg: array[1..az] of per;
    ko, kor: array[1..v3] of integer;
    tt: ^ttt;
    vt: array[1..abr, 1..ogr, 1..3] of 1..v;
    erk: array[2..v] of 1..az;
    ind: array[1..az] of 0..anz;
    fl: text;

 procedure initGruppen;
{   Erzeugt die Gruppen gl bzw. gr die vor links bzw. rechts operieren.   }
{   gl:=<(1,2,3,4,5,6,7)>  und  gr:=<(3,4,5,6,7)>}
    var
      i, j: integer;
 begin
    for i := 1 to ogr do
      for j := 1 to v do
        gr[i, j] := j;
    for i := 1 to ogl do
      for j := 1 to v do
        gl[i, j] := j;
    for i := 1 to ogl do
      for j := 1 to ogl do
        gl[i, j] := (i + j - 2) mod ogl + 1;
    for i := 1 to ogr do
      for j := 1 to ogr do
        gr[i, j + 2] := (i + j - 2) mod ogr + 1 + 2;
 end;

 procedure initBahn;
    var
      i1, i2, i3, x, i, j, l: integer;
 begin
{   tu numeriert die ungeordneten 3-Mengen.   }
{   nttu liefert zu jeder Nummer ein Vertreter der 3-Menge.   }
    l := 0;
    for i3 := 3 to v do
      for i2 := 2 to i3 - 1 do
        for i1 := 1 to i2 - 1 do
          begin
            l := l + 1;
            tu[i1, i2, i3] := l;
            tu[i1, i3, i2] := l;
            tu[i2, i1, i3] := l;
            tu[i2, i3, i1] := l;
            tu[i3, i1, i2] := l;
            tu[i3, i2, i1] := l;
```

```
            nttu[l, 1] := i1;
            nttu[l, 2] := i2;
            nttu[l, 3] := i3;
          end;
{   bahnl ordnet jeder (Nummer einer) 3-Menge eine Bahn von gl auf den 3-Mengen zu    }
{   ko zählt die nichtregularität d.h. wie oft eine 3-Menge durch gl auf sich abgebildet wird }
    for i := 1 to v3 do
      ko[i] := 0;
    l := 0;
    for i := 1 to v3 do
      if ko[i] = 0 then
        begin
          l := l + 1;
          for j := 1 to ogl do
            begin
              x := tu[gl[j, nttu[i, 1]], gl[j, nttu[i, 2]], gl[j, nttu[i, 3]]];
              ko[x] := ko[x] + 1;
              bahnl[x] := l;
            end;
        end;
{   Dasselbe wie oben für gr.    }
{   vt ordnet jeder Bahn die darinliegenden 3-Mengen mit Vielfachheit zu }
    for i := 1 to v3 do
      kor[i] := 0;
    l := 0;
    for i := 1 to v3 do
      if kor[i] = 0 then
        begin
          l := l + 1;
          for j := 1 to ogr do
            begin
              x := tu[gr[j, nttu[i, 1]], gr[j, nttu[i, 2]], gr[j, nttu[i, 3]]];
              kor[x] := kor[x] + 1;
              bahnr[x] := l;
              vt[l, j, 1] := gr[j, nttu[i, 1]];
              vt[l, j, 2] := gr[j, nttu[i, 2]];
              vt[l, j, 3] := gr[j, nttu[i, 3]];
            end;
        end;
  end;

  function get (a: per): tet;
{   Liefert zu dem Erzeuger a die Daten Struktur, die für jedes Element aus der Bahn der }
{   Spalten die Anzahl der darin vorkommenden Bahnen von Einträgen enthält, nämlich: }
{   t[i, 0].a ist die Anzahl der verschiedenen Bahnen von Einträgen in der Bahn i der Spalten. }
{   Für 1≤k≤t[i, 0].a steht in t[i, k].x die (Nummer der) k-ten Bahnen von Einträgen in der in der }
{   Bahn i der Spalten vorkommt. In t[i, k].a steht die Vielfachheit des Auftretens von t[i, k].x }
    label
      100;
    var
      i, j, k, x: integer;
      t: tet;
  begin
    for i := 1 to abr do
      t[i, 0].a := 0;
    for i := 1 to abr do
      for j := 1 to ogr do
        begin
```

```
          x := bahnl[tu[a[vt[i, j, 1]], a[vt[i, j, 2]], a[vt[i, j, 3]]]];
          for k := 1 to t[i, 0].a do
            if t[i, k].x = x then
             begin
              t[i, k].a := t[i, k].a + 1;
              goto 100;
             end;
          t[i, 0].a := t[i, 0].a + 1;
          t[i, t[i, 0].a].a := 1;
          t[i, t[i, 0].a].x := x;
100:
        end;
    get := t;
 end;

  procedure initper (ti: integer);
{   Erzeugt alle möglichen Vertreter von Zeilen die der Normierung nach Bsp.(3.26) genügen  }
{   und speichert diese in ap^ und, die zugehörige in "get" beschriebene Datenstrukur, in tt^ ab.  }
{   Dabei werden die Vertreter und ihre Daten mittels "erk" in drei Gruppen eingeteilt, die  }
{   durch die Bahnen ihrer ersten Beiden Elemente unter gl gegeben sind (siehe (3.26).  }
    label
      100;
    var
      i, j, x: integer;
 begin
    if ti = v + 1 then
     begin
        x := erk[a[2]];
        if (x <> 1) | ((a[2] = 7) & (a[4] = 3)) then
         begin
            ind[x] := ind[x] + 1;
            ap^[x, ind[x]] := a;
            tt^[x, ind[x]] := get(a);
         end;
     end
    else
     for i := 3 to v do
        begin
         for j := 2 to ti - 1 do
            if a[j] = i then
              goto 100;
         a[ti] := i;
         if ti = 2 then
            initper(4)
         else
            initper(ti + 1);
100:
        end;
 end;

  procedure init;
{   Initialisiert die Datenstruktur kon[i, j], die das vorkommen einer Bahn i von Einträgen  }
{   in einer Bahn j von Spalten zählt. Dies geschieht so, daß wenn kon[i, j] den Wert la  }
{   erreicht, die Benötigten Vertreter der Bahn i in der Bahn j, unter Berücksichtigung  }
{   eventueller Nichtregularitäten, alle vorhanden sind. }
    var
      i1, i2, i3, i, j: integer;
 begin
```

```
    for i := 1 to abl do
     for j := 1 to abr do
        kon[i, j] := la - la div (ko[i] * kor[j]);
 end;

  procedure wrt;
{   Druckt das Ergebnis   }
    var
      i, j: integer;
 begin
    for i := 1 to az do
     begin
        for j := 1 to v do
          write(erg[i, j] : 3);
        writeln;
     end;
    writeln;
 end;

  procedure rt (ti: integer);
{   Diese Prozedur überprüft ob sich ein Vertreter für die ti-te Zeile des Erzeugendensystems  }
{   zu den bisher gefundenen hinzufügen läßt, ohne daß die Bedingung verletzt wird, daß in jeder }
{   Bahn der Spalten jede Bahnen von Einträgen la-mal vorkommt (vgl. dazu init). Ist ein solcher
}
{   Vertreter gefunden versucht man, durch rekursiven Aufruf derselben Prozedur, einen   }
{   Vertreter für die nächste Zeile des Erzeugendensystems zu finden bis man alle az Zeilen,  }
{   sofern existent, gefunden hat.   }
    label
      100;
    var
      i, j, k: integer;
 begin
    if ti = az + 1 then
     begin
{   Man hat alle Zeilen des Erzeugendensystems gefunden.  }
{   Man läßt das Erzeugendensystems ausdrucken und hält das Programm an.  }
        wrt;
        halt;
     end
    else
     begin
        for i := 1 to ind[ti] do
{   Mit dieser Schleife läuft man durch alle Vertreter der ti-ten Zeile, }
{   die in initper erzeugt wurden.  }
          begin
            for j := 1 to abr do
              for k := 1 to tt^[ti, i, j, 0].a do
              if kon[tt^[ti, i, j, k].x, j] + tt^[ti, i, j, k].a > la then
              goto 100;
{   Hier wurde kontrolliert ob die Zeile sich zufügen läßt ohne die Bedingung, daß in jeder Bahn  }
{   der Spalten jede Bahnen von Einträgen la-mal vorkommt, zu verletzen.  }
{   Ist die Bedingung nicht erfüllt wird der nächste Vertreter getestet, sonst fügt man die Zeile }
{   hinzu (diese wird in "erg" gespeichert) und ruft die Prozedur rekursiv auf um dasselbe für  }
{   die nächste Zeile zu testen.  }
            for j := 1 to abr do
              for k := 1 to tt^[ti, i, j, 0].a do
               kon[tt^[ti, i, j, k].x, j] := kon[tt^[ti, i, j, k].x, j] + tt^[ti, i, j, k].a;
            erg[ti] := ap^[ti, i];
```

```
            rt(ti + 1);
            for j := 1 to abr do
              for k := 1 to tt^[ti, i, j, 0].a do
               kon[tt^[ti, i, j, k].x, j] := kon[tt^[ti, i, j, k].x, j] - tt^[ti, i, j, k].a;
{   Lies sich eine Ebene höher kein weiter Vertreter zufügen, so nimmt man die, in dieser Ebene }
{   hinzugefügte Zeile, wieder weg und versucht es mit dem nächsten Vertreter. }
100:
         end;
      end;
 end;


begin
  new(ap);
   new(tt);

  initGruppen;
  initBahn;
   init;

  a[1] := 1;
  a[3] := 2;
  erk[2] := 1;
  erk[7] := 1;
  erk[3] := 2;
  erk[6] := 2;
  erk[4] := 3;
  erk[5] := 3;
{   erk[i] ist die Nummer der Bahn der Menge (1,i) unter gl . Diese wird benutzt um die  }
{   Vertreter der Doppelnebenklasse zu ordnen vergleiche (3.26)  }
   initper(2);

   rt(1);
end.
```

## Programm zu Beispiel (3.27)

```
program DNK;
{  Gesucht wird ein PA2(2,v,v) der Form G∪GaG, mit G Gruppe der Ordnung og.  }
 const
    v = 12;
    og = v - 1;
    n = v - 2;
    n2 = (v - 1) * (v - 2) div 2;
    ab = n div 2;

 type
    per = array[0..n] of 0..n;
    grt = array[0..n] of per;
    tut = array[0..n, 0..n] of 0..n2;
    ntut = array[1..n2, 1..2] of 0..n;
    bahnt = array[0..n2] of 0..ab;
    anzahlt = array[0..n2, 0..n2] of 0..2;

 var
    i, j, k: integer;
    gr: grt;
    tu: tut;
    nttu: ntut;
    bahn: bahnt;
    anzahl: anzahlt;
    a: per;

 procedure initgr;
{  Erzeugt eine zyklische Gruppe gr der Ordnung og  }
{  gr=<(0,1,..,n)>}
    var
      i, j: integer;
 begin
    for i := 0 to n do
     for j := 0 to n do
        gr[i, j] := (i + j) mod og;
 end;

 procedure initbahn;
    var
      x, i, j, l: integer;
      ko: array[1..n2] of integer;
 begin
{  Gibt jedem ungeordneten Paar (i,j) verschiedener Einträge eine Nummer tu[i,j].  }
{  Zu jeder Nummer wird ein Vertreter nttu des ungeordneten Paares erzeugt.  }
    l := 0;
    for i := 1 to n do
     for j := 0 to i - 1 do
        begin
         l := l + 1;
         tu[i, j] := l;
         tu[j, i] := l;
         nttu[l, 1] := i;
         nttu[l, 2] := j;
        end;
```

```
{   Gibt den (unerwünschten) Paaren (i,i) und Ihrer Bahn die Nummer 0  }
    for i := 0 to n do
      tu[i, i] := 0;
    bahn[0] := 0;
{   Liefert die Tabelle "bahn" die jeder (Nummer eines) ungeordneten Paaren seine Bahn  }
{   unter gr zuordnet  }
    for i := 1 to n2 do
      ko[i] := 0;
    l := 0;
    for i := 1 to n2 do
      if ko[i] = 0 then
        begin
          l := l + 1;
          for j := 0 to n do
            begin
              x := tu[gr[j, nttu[i, 1]], gr[j, nttu[i, 2]]];
              ko[x] := ko[x] + 1;
              bahn[x] := l;
            end;
        end;
 end;

  procedure initanzahl;
    var
      i, j: integer;
 begin
{   Initialisiert den Zähler auf 0 bis auf für die Paare vom Typ 0 die nicht vorkommen sollen, }
{   und deren Zähler deshalb auf die Maximalanzahl 2 gesetzt werde. Für die Bahnen die schon }
{   im ersten Teil der Konstruktion (gr) einmal vorkamen, wird der Zähler auf 1 gesetzt  }
    for i := 1 to n2 do
      for j := 1 to n2 do
        anzahl[i, j] := 0;
    for i := 0 to n2 do
      anzahl[i, 0] := 2;
    for i := 1 to n2 do
      anzahl[i, i] := 1;
 end;

  procedure rt (ti: integer);
{   In dieser Prozedur wird versucht an das schon vorhandene Anfangsstück der erzeugenden }
{   Permutation ein weiteres Element Anzuhängen}
    label
      100;
    var
      i, j, jj, x, y: integer;
 begin
    if ti = n + 1 then
      begin
{Wir haben die erzeugende Permutation vollständig bestimmt und drucken sie. }
        write(0 : 3, -1 : 3);
        for j := 1 to n do
          write(a[j] : 3);
        writeln;
      end
    else
      begin
        for i := 1 to n do
{   Die Schleife lauft über alle möglichen Elemente der Grundmenge. Dieses Element versuchen  }
```

```
{   wir an das Anfangsstück der erzeugende Permutation anzuhängen.  }
        begin
          for j := 1 to ti - 1 do
           begin
             if anzahl[bahn[tu[ti, j]], bahn[tu[i, a[j]]]] = 2 then
{   Hier wird überprüft ob durch das zufügen des neuen Elements an den bis jetzt gefundenen  }
{   Teil der Erzeugenden Permutation ein Widerspruch entsteht zu der Bedingung, daß in dem }
{   Spaltenpaar (j,ti) jedes Eintragspaar nur 2 mal vorkommen darf (ti ist die aktuelle Spalte). }
{   Dabei wird durch die Initialisierung des Zählers auch erreicht, daß man kein Element zweimal }
{   einfügt. Ist das zufügen des Elements möglich so wird der Zähler entsprechend erhöht. Wird }
{   die Bedingung verletzt so macht man alle bisherigen Erhöhungen des Zählers in dieser Schleife}
{   rückgängig und springt aus der Schleife, so daß der Versuch mit dem nächsten Element  }
{   wiederholt  wird.}
             begin
              for jj := 1 to j - 1 do
                 anzahl[bahn[tu[ti,jj]],bahn[tu[i,a[jj]]]]:=anzahl[bahn[tu[ti,jj]],bahn[tu[i,a[jj]]]]-1;
              goto  100;
             end;
               anzahl[bahn[tu[ti, j]], bahn[tu[i, a[j]]]]:=anzahl[bahn[tu[ti, j]], bahn[tu[i, a[j]]]]+1;
            end;
{   Lies sich daß Element einfügen ohne die Bedingung zu verletzen so verlängert man das  }
{   Anfangsstück der erzeugenden Permutation um dieses Element und ruft diese Prozedur}
{   Rekursiv  wieder  auf.}
          a[ti]  :=  i;
          rt(ti  +  1);
{   Ist es, in einer Ebene höher nicht gelungen das Anfangsstück zu ergänzen, so macht man  }
{   die in dieser Ebene am Zähler gemachten Änderungen rückgängig und versucht es mit dem  }
{   nächsten Element.  }
          for j := 1 to ti - 1 do
            anzahl[bahn[tu[ti, j]], bahn[tu[i, a[j]]]] := anzahl[bahn[tu[ti, j]], bahn[tu[i, a[j]]]] - 1;
100:
        end;
     end;
 end;

begin
  initgr;
 initbahn;
 initanzahl;
  rt(1);
end.
```

# Literaturverzeichnis


[1] T.Beth, D.Jungnickel, H.Lenz: *Design Theory*, Bibliographiches Institut Zürich (1985).

[2] J.Bierbrauer: *Monotypical uniformly homogeneous Sets of Permutations*, Archiv der Mathematik 58(1992) 338-344.

[3] J.Bierbrauer: *The uniformly 3-homogeneous subsets of $PGL_2(q)$*, Manuskript 1992.

[4] J.Bierbrauer: *A Family of Perpendicular Arrays achieving perfect 4-fold Secrecy*, Manuskript 1992.

[5] J.Bierbrauer, Y.Edel: *Halving $PSL_2(q)$*, Manuskript 1992.

[6] J.Bierbrauer, Y.Edel: *Theory of perpendicular arrays*, eingereicht an: Journal of Combinatorial Designs 1993.

[7] J.Bierbrauer, T.v.Trung: *Halving $PGL_2(2^f)$ f odd a Series of Cryptocodes*, Designs Codes and Cryptography 1(1991) 141-148.

[8] J.Bierbrauer, T.v.Trung: *Some highly symmetric Authentication Perpendicular Arrays*, Designs, Codes and Cryptography (1992) 307-319.

[9] A.L.Dulmage, D.Johnson, N.S.Mendelson: *Orthomorphisms of groups and orthogonal Latin squares* , I. Canadian J. Math. 13(1961) 356-372.

[10] A.Granville, A.Moisiadis, R.Rees: *Nested Steiner n-cycle Systems and perpendicular Arrays*, Journal of Comb Math and Comb Comput. 3(1988) 163-167.

[11] H.Hanani: *Truncated finite planes*, Proc. Symposia in Pure Mathematics, AMS 19(1971) 115-120.

[12] H.Hanani, A.Hartman, E.S.Kramer: *On three-designs of small order*, Discrete Mathematics 45 (1983) 75-97.

[13] B.Huppert: *Endliche Gruppen I*, Springer Berlin (1967).

[14] W.M.Kantor: *On incidence matrices of finite projective and affine spaces*, Mathematische Zeitschrift 124(1972) 315-318.

[15] E.S.Kramer, D.L.Kreher, R.Rees, D.R.Stinson: *On perpendicular Arrays with $t \geq 3$*, Ars Combinatoria 28(1989) 215-223.

[16] C.C.Lindner: *Perpendicular Arrays and Graph Decompositions*, Ars Combinatoria 26B(1988) 67-92.

[17] C.C.Lindner, R.C.Mullin, G.H.J.van Rees: S*eparable Orthogonal Arrays*, Utilitas Mathematica 31(1987), 25-32.

[18] C.C.Lindner, D.R.Stinson: *The Spectrum for the Conjugate Invariant Subgroups of Perpendicular Arrays,* Ars Combinatoria 18(1983) 51-60.

[19] C.C.Lindner, D.R.Stinson:*Steiner Pentagon Systems*,Discrete Mathematics 52(1984), 67-74.

[20] R.C.Mullin, P.J.Schellenberg, G.H.J.van Rees, S.A. Vanstone: *On the construction of Perpendicular Arrays*, Utilitas Mathematica 18(1984), 141-160.

[21] C.R.Rao: *Combinatorial Arrangements analogous to Orthogonal Arrays,* Sankhya A23(1961), 283-286.

[22] P.J.Schellenberg, G.H.J.van Rees, S.A. Vanstone: *Four pairwise orthogonal latin squares of order 15,* Ars Combinatoria 6(1978) 141-150.

[23] D.R.Stinson: *The Spectrum of nested Steiner Tripel Systems*, Graphs and Combinatorics 1(1985) 189-191.

[24] D.R.Stinson: *On the Spectrum of nested 4-cycle Systems*, Utilitas Mathematica 33(1988) 47-50.

[25] D.R.Stinson: *Some Constructions and Bounds for Authentication Codes*, Journal of Cryptology 1(1988) 37-51.

[26] D.R.Stinson: *A Construction for Authentication/Secrecy Codes from certain Combinatorial Designs*, Journal of Cryptology 1(1988) 119-127.

[27] D.R.Stinson: *The Combinatorics of Authentication and Secrecy Codes*, Journal of Cryptology 2 (1990) 23-49

[28] D.R.Stinson, L.Teirlinck: *A Construction for Authentication/Secrecy Codes from 3-homogeneous Permutation Groups*, European Journal of Combinatorics 11(1990) 73-79.

[29] L.Teirlinck: *On large Sets of disjoint orderd Designs,* Ars Combinatoria 25(1988) 31-37.

[30] L.Tierlinck:*Large Sets of Disjoint Designs and Related Sructures*, Contemporary Design Theory: A Collection of Surveys, edited by J.H.Dinitz and D.R.Stinson, Wiley 1992.

[31] D.T.Todorov: *Three Mutually Orthogonal Latin Squares of Order 14*, Ars Combinatoria (1985) 45-48.

[32] T.v.Trung: *On the Construction of Authentication and Secrecy Codes*, Universität GH Essen Preprint Series 17(1991).

[33] R.M.Wilson: *An existence theory for pairwise balanced designs III* , Journal of Combinatorial Theory A 18(1975) 71-79.

[34] R.M.Wilson: *Inequaleties for t-Designs,* Journal of Combinatorial Theory A 34(1983) 313-324.