Gerhard Zauner

Orthogonale Lateinische Quadrate und Anordnungen, Verallgemeinerte Hadamard-Matrizen und Unabhängigkeit in der Quanten-Wahrscheinlichkeitstheorie

Diplomarbeit zur Erlangung des Akademischen Grades Magister der Naturwissenschaften Studienrichtung Mathematik Universität Wien

Begutachter:

PROF. DR. JOHANN CIGLER

" Der Witz hascht näher oder ferner vom Ende eine Ähnlichkeit, und der Verstand prüft sie und findet sie richtig..."

G. Ch. Lichtentenberg, Sudelbücher F 1186

Vorwort

Kombinatorische Designs lassen sich nach W.D. Wallis [47] generell charakterisieren als "to be a way of selecting subsets from a finite set in such a way that some specified conditions are satisfied." Die folgende Untersuchung zeigt anhand spezieller Strukturen die Möglichkeit einer Verallgemeinerung der Design Theorie auf, in welcher die endliche Menge durch einen endlichdimensionalen, komplexen Vektorraum ersetzt wird, aus dem lineare Teilräume ausgewählt werden sollen, die bestimmte Bedingungen erfüllen. Den linearen Teilräumen des \mathbb{C}^n lassen sich eindeutig (darauf projizierende) orthogonale n×n Projektionsmatrizen zuordnen. Diese werden die eigentlichen Grundelemente der Theorie bilden.

Den dieser Arbeit zugrundeliegenden Problemen der (klassischen)
Design Theorie, wie z.B. der Bestimmung paarweise orthogonaler
Lateinischer Quadrate, bzw. allgemeiner Orthogonaler Anordnungen
der Stärke 2 (orthogonal arrays, siehe z.B. Raghavarao [36], Kap.
2), ist gemeinsam, daß sie zu einer wahrscheinlichkeitstheoretischen Aufgabe äquivalent sind, nämlich bestimmte bezüglich der
Gleichverteilung paarweise unabhängige Zufallsvariablen über einer
endlichen Menge aufzufinden. Diese Beobachtung war Ausgangspunkt
vorliegender Arbeit, zusammen mit der Entdeckung von Strukturen im
Rahmen der Quantentheorie, die sich unter Verwendung der üblichen
wahrscheinlichkeitstheoretischen Interpretation des Hilbertraumformalismus als natürliche Verallgemeinerung obiger Problemstellung
erkennen ließen.

Die zentrale Definition dieser Arbeit wird also in Kapitel 2 aus einer Untersuchung des Begriffs der Unabhängigkeit in der Wahrschein-

lichkeitstheorie, die der Quantentheorie zugrundeliegt, abgeleitet (ohne dabei andere als nur funktionalanalytische Vorkenntnisse vorauszusetzen). Speziell konzentriert sich diese Arbeit dann auf endlichdimensionale Hilberträume und das Problem paarweise bezüglich der normierten Einheitsmatrix unabhängige, selbstadjungierte, komplexe Matrizen zu bestimmen.

Die oben angeführten Probleme der klassischen Design Theorie sind hierbei nun zum Spezialfall von paarweise kommutierenden Matrizen äquivalent. Es zeigt sich, daß eine Reihe dafür charakteristischer Eigenschaften auch für den nichtkommutativen Fall gelten: Eine Verallgemeinerung einer klassischen Ungleichung führt zur Definition von vollständigen Systemen. Spezielle Konstruktionen dafür in Vektorräumen mit Primzahlpotenzordnung umfassen klassische vollständige Systeme (etwa von paarweise orthogonalen Lateinischen Quadraten) als Teillösungen. Zugleich ist die in Abschnitt 4.2 angegebene Ableitung selbst verwandt zu entsprechenden klassischen Konstruktionen, indem der Ausgangspunkt ebenfalls die Struktur der Unterräume von Vektorräumen über endlichen Körpern ist. Andererseits legen die Ergebnisse von Kapitel 5 z.B. die Nichtexistenz einer bestimmten Lösung im ℃ nahe, welche in natürlicher Weise als Gegenstück zur schon von L. Euler vermuteten und erst 1900 bewiesenen Nichtexistenz zweier orthogonaler Lateinischer 6×6 Quadrate angesehen werden kann.

Der dieser Arbeit zugrundeliegende Problemkomplex konnte nur ansatzweise behandelt werden und läßt noch viel Raum für weitere Untersuchungen. Bereits einleitend wurde darauf hingewiesen, daß er zugleich als Teil einer umfangreichen verallgemeinerten Design Theorie verstanden werden kann. Im Rest dieses Vorworts soll nun noch ein kurzer Ausblick darauf versucht werden.

Die in der Definition obiger Strukturen wesentlichen Größen sind die Spur: $\operatorname{tr}(P)$ einer orthogonalen Projektionsmatrix P, welche die Dimension des zugeordneten linearen Teilraums mißt, sowie: $\operatorname{tr}(PQ)$ als Maß der Gemeinsamkeit zweier orthogonaler Projektionsmatrizen P und Q (bzw. der zugeordneten Teilräume).

Wir wollen ein einfaches aber wichtiges Beispiel anführen, wie sich damit analog zu den Strukturen dieser Arbeit weitere verallgemeinerte (Projektor-) Designs in komplexen Vektorräumen definieren lassen:

Eine Menge von v komplexen, orthogonalen b×b Projektionsmatrizen: P.,...,P. soll "balanciertes Projektordesign" heißen, falls es ein r∈N und k,λ∈Q gibt, sodaß gilt:

$$i) P_i + \dots + P_v = k1$$

ii)
$$\operatorname{tr}(P_i) = r$$
 für alle $1 \le i \le v$
iii) $\operatorname{tr}(P_i P_j) = \lambda$ für alle $1 \le i \ne j \le v$

Die erste Bedingung ist eine Art Homogenitätsforderung. Eine Lösung aus kommutierenden Matrizen ist, ähnlich wie für obige Strukturen, äquivalent zu einem klassischen Design, nämlich einem sogenannten "balanced incomplete block design" (BIBD - darum die spezielle Wahl der Parameter). Dies sieht man, indem man die Diagonaleinträge von gleichzeitig diagonalisierten P.,...,P. jeweils als Indikatorfunktionen von Teilmengen der b-elementigen Menge aller Diagonalpunkte interpretiert. Die Bedingungen i)→iii) bezogen auf dieses Teilmengensystem sind, wie sich leicht nachprüfen läßt, genau die dualen Bedingungen von BIBD's (dual-siehe Wallis [47], p.26). Wieder übertragen sich viele Eigenschaften auf den nichtkommutativen Fall. Durch Anwendung der Spur auf i) bzw. Multiplikation von i) mit einem P,, ₄≤ί≤∨ und anschließender Anwendung der Spur erhält man mit ii) und iii) z.B.:

$$vr = bk$$

$$r(k-1) = \lambda(v-1)$$

Diese für BIBD's wohlbekannten Gleichungen sind also allgemein gültig. Aus ii) und iii) folgt für r≭b weiters sehr einfach, daß die b×b Projektionsmatrizen P_1, \ldots, P_v linear unabhängig im b^2 -dimensionalen Vektorraum aller b×b Matrizen sind. Also gilt v≤b² und für kommutierende Matrizen v≤b. Letztere ist als Ungleichung von Fisher für BIBD's bekannt. Die Lösungen und ihre Eigenschaften wurden bislang nur zu einem kleinen Teil untersucht.

Eine sytematische Untersuchung aller analog möglichen Verallgemeinerungen von Konzepten der klassischen Design Theorie und ihrer Zusammenhänge ist erst noch zu leisten. Deren Lösungen sind natürlich viel umfangreicher und komplizierter als jene klassischer Designs, welche als Spezialfälle für kommutierende Matrizen enthalten sind. Da diese Arbeit aber an Beispielen zeigt, daß sich eine Reihe von deren Eigenschaften im nichtkommutativen Fall wiederfinden, teilweise auch in neuen Zusammenhängen, ist nicht ausgeschlossen, daß die Analyse der verallgemeinerten Theorie auch Hinweise oder Anregungen für die klassische Theorie liefert. Als Anwendung bieten sich natürlich vor allem, wie in Kapitel 2 und 6 dieser Arbeit, grundsätzliche Probleme in der Quantentheorie an.

Die vorliegende Untersuchung ist also nur ein erster, vorläufiger Beitrag zu einer verallgemeinerten Design Theorie. Aufbau und Form spiegeln (mit den ihnen anhaftenden Unzulänglichkeiten) den Entstehungsprozeβ der Ideen wieder.

Wien, April 1991

G. Zauner

Herrn Professor Dr. J. Cigler möchte ich herzlich für die Bereitschaft diese Arbeit entgegenzunehmen und die Mühe der Durchsicht danken.

Inhaltsverzeichnis:

1	Einleitung	
2	Unabhängigkeit	15
3	Äquivalenzen, Schranken	31
4	Vollständige Systeme	43
5	VBH-Matrizen, VH-Matrizen und deren Produkte	62
6	Anwendungen	76
Li	teraturverzeichnis	79

1. EINLEITUNG

Eine Darstellung der Wahrscheinlichkeitstheorie, die der Quantenmechanik zugrunde liegt, erfolgt erst im nächsten Kapitel. Hier wird einleitend vorerst ein klassisches wahrscheinlichkeitstheoretisches Modell und dessen Verbindung zu kombinatorischen Themen diskutiert. Die für diese Arbeit zentrale Definition 1.1 wird dann als eine natürliche Verallgemeinerung hiervon vorgestellt. Eine andere Formulierung führt zu Def.1.2 und zu weiteren relevanten Strukturen und Ansätzen. Damit ist das mathematische Umfeld umrissen. Es schließt sich noch ein kurzer Überblick der weiteren Kapitel und erzielten Ergebnisse an.

1.1 KLASSISCHE UNABHÄNGIGKEIT, LATEINISCHE QUADRATE, ETC.

Betrachten wir als Ausgangspunkt folgendes Problem: Gegeben sei eine n-elementige Menge $\Omega = \{\omega_1, \ldots, \omega_n\}$ mit gleichverteiltem Wahrscheinlichkeitsmaß: $\mu(\omega_i) = \frac{1}{n}$ für alle $1 \le i \le n$. Bekanntlich heißen zwei (diskrete) Zufallsvariablen $\mathbf{f}_1, \mathbf{f}_2: \Omega \to \mathbb{R}$ unabhängig, falls:

$$\mu\left[\mathbf{f_{i}^{-i}}\left(\boldsymbol{\chi_{i}}\right)\ \cap\ \mathbf{f_{2}^{-i}}\left(\boldsymbol{\chi_{2}}\right)\right] = \mu\left[\mathbf{f_{i}^{-i}}\left(\boldsymbol{\chi_{i}}\right)\right], \mu\left[\mathbf{f_{2}^{-i}}\left(\boldsymbol{\chi_{2}}\right)\right]$$

für beliebige x_i aus dem Wertebereich von f_i , i=1,2. Sei mit |A| die Mächtigkeit der Menge A bezeichnet, so folgt hier:

$$|\mathbf{f}_{4}^{-1}(\mathbf{x}_{4})| \cap \mathbf{f}_{2}^{-1}(\mathbf{x}_{2})| = \frac{1}{2} |\mathbf{f}_{4}^{-1}(\mathbf{x}_{4})|, |\mathbf{f}_{2}^{-1}(\mathbf{x}_{2})|$$
 (1.1)

Gesucht sind alle k-tupel $\mathbf{f_1}, \mathbf{f_2}, \dots, \mathbf{f_k}$ paarweise unabhängiger Zufallsvariablen.

Sei etwa n = p.q und die Elemente von $\Omega = \{\omega_{i,j}: 1 \le i \le p, 1 \le j \le q\}$ mit neuen Indizes versehen, so sind für beliebige reellwertige Funktionen $g_i: \{1,\dots,p\} \to \mathbb{R}$ und $g_2: \{1,\dots,q\} \to \mathbb{R}$

$$\mathbf{f}_{\mathbf{i}}(\omega_{i,j}) := \mathbf{g}_{\mathbf{i}}(i) \quad \text{und} \quad \mathbf{f}_{\mathbf{z}}(\omega_{i,j}) := \mathbf{g}_{\mathbf{z}}(j) \quad (1.2)$$

unabhängig. Sogar alle Paare bzgl. μ unabhängiger Zufallsvariablen ${\bf f_1,f_2}$ lassen sich durch Umordnen von Ω auf diese Gestalt bringen.

Der Beweis ist kurz: Die Urbilder der verschiedenen Werte von $\mathbf{f_1}$ und $\mathbf{f_2}$ geben jeweils eine Partition von Ω in disjunkte Teilmengen. Seien deren Mächtigkeiten k_i , $1 \le i \le r$ und l_j , $1 \le j \le s$. Aus Formel (1.1) folgt, daß der Durchschnitt einer Menge mit k_i Elementen und einer Menge mit l_j Elementen genau $k_i l_j / n \in \mathbb{N}$ Elemente hat. Sei $k = ggT(k_1, \ldots, k_r)$ und $l = ggT(l_1, \ldots, l_s)$. Da $n \mid k_i l_j$ für alle $1 \le i \le r$, $1 \le j \le s$ und k l eine Linearkombination der $k_i l_j$ ist, folgt $n \mid k l$. Also gibt es $p,q \in \mathbb{N}$, sodaß n = pq und $q \mid k \Rightarrow q \mid k_i$, für alle $1 \le i \le r$, sowie $p \mid l \Rightarrow p \mid l_j$, für alle $1 \le j \le s$. Da also die Anzahl der Punkte, wo $\mathbf{f_1}$ jeweils konstant ist, immer Vielfaches von q ist, läßt sich durch geeignetes Umordnen von $\Omega = (\omega_{i,j}, 1 \le i \le p, 1 \le j \le q)$ ein $\mathbf{g_1}(i)$ definieren dem $\mathbf{f_1}$ entspricht. Es ist auch sofort klar, daß dasselbe gleichzeitig für $\mathbf{f_2}$ und ein passen-

Schwieriger ist das Problem für k≥3: Nehmen wir zum Beispiel an, daß n=r² ist und die k paarweise unabhängigen Zufallsvariablen jeweils genau r verschiedene Werte besitzen. Dieses Problem ist äquivalent zur Bestimmung von k-2 paarweise orthogonalen Lateinischen r×r Quadraten, wie wir nun zeigen:

des g₂(j) möglich ist.

Seien o.B.d.A. die r verschiedenen Werte jeweils: 0,...,r-1. Deren Urbilder sind also immer nicht leer: $|\mathbf{f}_i^{-1}(\iota)| \neq \emptyset$ für alle o $\leq \iota \leq r-1$. Mit Glchg.(1.1) folgt dann für zwei verschiedene \mathbf{f}_i und \mathbf{f}_j ($\iota \neq j$):

$$|f_i^{-1}(l) \cap f_i^{-1}(m)| \neq \emptyset$$
 für alle o $\leq l \leq r-1$, o $\leq m \leq r-1$

Die Durchschnitte ihrer verschiedenen Urbilder sind also genau $r^2=n$ nichtleere und natürlich disjunkte Teilmengen der n-elementigen Menge Ω . Es folgt, daß sie alle ein-elementig sein müssen. Die Urbilder $\mathbf{f}_{i}^{-1}(\iota)$, $o \le \iota \le r-1$ sind folglich jeweils genau r-elementig. Mit dem obigen können wir o.B.d.A. ansetzen:

$$\Omega \; = \; \left\{ \boldsymbol{\omega}_{i,j} \; : \; 1 \leq i \leq r \; , \; \; 1 \leq j \leq r \right\} \quad \; \text{ und } \quad \; \boldsymbol{f}_{\underline{i}} \; (\boldsymbol{\omega}_{i,j}) = \underline{i} - 1 \; , \quad \; \boldsymbol{f}_{\underline{2}} \; (\boldsymbol{\omega}_{i,j}) = \underline{j} - 1 \; .$$

Mit den restlichen Zufallsvariablen $\mathbf{f_3}, \ldots, \mathbf{f_k}$ können nun r×r Matrizen $\mathbf{L^{(m)}}, \mathbf{g} \leq \mathbf{m} \leq \mathbf{k}$, mit Einträgen: $\mathbf{l_{ij}^{(m)}} := \mathbf{f_m}(\omega_{ij})$ definiert werden. Diese müssen dann nach den vorigen Überlegungen in jeder Spalte und Zeile jeden Wert: $0, \ldots, r-1$ genau einmal stehen haben und übereinandergelegt jedes geordnete Wertepaar genau an einer Stelle annehmen.

Dies entspricht genau der Definition von k-2 Lateinischen Quadraten und ihrer paarweisen Orthogonalität. (Standardreferenz dazu: Dénes/Keedwell [20]). Für welche k diese genau existieren ist allgemein nicht bekannt. Es gibt aber spezielle Konstruktionen und Abschätzungen.

So beweisen wir in Kap.3, daß für k paarweise bzgl. der Gleichverteilung unabhängige Zufallsvariablen $\mathbf{f_i}, \ldots, \mathbf{f_k}$ über einer n-elementigen Menge, wobei $\mathbf{r_i}$ die Anzahl der verschiedene Werte von $\mathbf{f_i}$ sei, gilt:

 $1 - k + \sum_{i=1}^{k} r_{i} \le n \tag{1.3}$

Im vorigen Beispiel mit $n=r^2$ und $r_i=r$ $\forall i$ folgt daraus die bekannte Schranke $k \le r+1$, d.h. es gibt maximal r-1 paarweise orthogonale Lateinische $r \times r$ Quadrate.

Eine Verallgemeinerung orthogonaler Lateinischer Quadrate sind "Orthogonale Anordnungen" (orthogonal arrays – siehe Bose/Bush [08] oder Raghavarao [36], Kap.2).

Eine orthogonale Anordnung OA(n,k,r,2) von Größe n, Grad k, r Elementen, Index λ und Stärke 2 ist eine k*n Matrix mit r verschiedenen Elementen (üblicherweise: 0,1,...,r-1) als Einträgen, sodaß jede 2×n Submatrix jede mögliche Spalte genau λ mal enthält. Es folgt sofort, daß jeder der Einträge in jeder Zeile genau λ r mal stehen muß und also $n=\lambda r^2$ ist.

Interpretiert man die i-te Zeile dieser k×n Matrix als Funktion \mathbf{f}_i über einer n-elementigen Menge, so sieht man sofort die Äquivalenz zum Problem k paarweise bzgl. der Gleichverteilung unabhängige Zufallsvariablen über einer n-elementigen Menge zu bestimmen, welche jeweils genau \mathbf{r} verschiedene Werte und diese jeweils genau \mathbf{r} mal annehmen.

Gleichung (1.3) gibt wieder eine bekannte Schranke:

$$k \leq \frac{\lambda r^2 - 1}{r - 1}$$

Eine OA(n,k,r,2) mit $n=r^2$, d.h. Index $\lambda=1$ entspricht k-2 paarweise orthogonalen Lateinischen r×r Quadraten.

Nur eine andere Notation von OA's sind (s,r,μ) -Netze (Drake [21]), bzw. (als duale Struktur) Transversale Designs (siehe Beth/Jung-nickel/Lenz [07], Kap.I, \$7.)

Eine weitere Verallgemeinerung Lateinischer Quadrate, die auch unter die hier skizzierte Problemstellung fällt, wurde unter der Bezeichnung F-(=Frequenz)-Quadrate bzw. F-Rechtecke, und deren Orthogonalität untersucht. (Hedayat/Seiden [27], Federer/Mandeli [22]).

12. EINE VERALLGEMEINERUNG

Der Quantenmechanik liegt eine Erweiterung der klassischen Wahrscheinlichkeitstheorie zugrunde, in der das Tripel aus der Menge Ω , der σ -Algebra Σ und dem Maß μ ersetzt wird durch $(\mathscr{R},\mathcal{P},\mathcal{D})$: \mathscr{R} ist ein separabler Hilbertraum. $P \in \mathcal{P}$ sind die orthogonalen Projektionsoperatoren auf die (abgeschlossenen) Unterräume von \mathscr{R} . Normierte Maße werden durch sogenannte Dichteoperatoren $D \in \mathcal{D}$ beschrieben. Das sind positiv semidefinite Operatoren mit Spur trD=1. Das Maß einer orthogonalen Projektion P bzgl. D ist: $\mu_{D}(P):=tr(PD)$. Zufallsvariablen sind selbstadjungierte Operatoren.

Dieses Konzept wird in Kap.2 genauer beschrieben. Es wird die (in dieser Form scheinbar noch nirgends untersuchte) Unabhängigkeit selbstadjungierter Operatoren definiert. Im Großteil dieser Arbeit beschränken wir uns auf den \mathbb{C}^n . Eine besondere Rolle spielt dabei die Unabhängigkeit bzgl. der "Gleichgewichtsdichtematrix" $\mathbf{D} = \frac{1}{n}\mathbf{1}$. (1...Einheitsmatrix), bzw. dem durch sie erzeugten "homogenen" Maß. Dies führt zu der folgenden zentralen Definition:

1.1. **DEFINITION**: Zwei selbstadjungierte komplexe n×n Matrizen A und B mit Spektralzerlegung:

$$A = \sum_{i=1}^{r} a_i P_i \qquad \text{und} \qquad B = \sum_{j=1}^{n} b_j Q_j$$

wobei a_i , $4 \le i \le r$ und b_j , $4 \le j \le s$ die jeweils <u>verschiedenen</u> Eigenwerte aus \mathbb{R} , P_i und Q_j die assoziierten orthogonalen Projektionen auf die Eigenräume sind, heißen unabhängig bzgl. $\frac{4}{n}$ 1, falls :

$$tr(P_iQ_i) = \frac{1}{n}tr(P_i)tr(Q_i)$$
 (1.4)

für alle i≤i≤r und i≤j≤s gilt.

Da für festes j die Summe von (1.4) über alle i eine Identität ergibt und dasselbe für festes i und Summe über j gilt, sind (1.4) nur (r-1)(s-1) unabhängige Bedingungen. Um triviale Fälle auszuschließen verlangen wir in der Folge r≥2 und s≥2.

Das klassische Konzept von bzgl. der Gleichverteilung unabhängigen Zufallsvariablen über einer n-elementigen Menge ist als Spezialfall für kommutierende A und B enthalten:

Diese lassen sich durch eine unitäre Matrix \mathbf{U} , mittels $\mathbf{A} \to \mathbf{U}^{-1}\mathbf{A}\mathbf{U}$, $\mathbf{B} \to \mathbf{U}^{-1}\mathbf{B}\mathbf{U}$ gleichzeitig auf Diagonalform transformieren. (siehe z.B. Hoffman/Kunze [29] Kap. $\mathbf{9}$, Th $\mathbf{15}$). Diese Abb. ist mit Definition 1.1 verträglich. Interpretiert man nun die Diagonaleinträge der Matrizen jeweils als Werte von klassischen Zufallsvariablen über einer n-elementigen Menge (den Diagonalpunkten), so folgt die Äquivalenz der Gleichungen (1.1) und (1.4) sofort:

 P_i nimmt genau auf jenen Diagonalpunkten 1 an, wo A den Wert a_i stehen hat. $tr(P_i)$ gibt die Anzahl dieser Punkte (die Vielfachheit von $a_i)$ an. Dasselbe gilt für $tr(Q_j)$ und b_j . P_iQ_j hat Einsen genau auf dem Durchschnitt dieser Mengen und $tr(P_iQ_j)$ gibt dessen Mächtigkeit an.

Damit lassen sich z.B. die einleitenden Überlegungen, daß sich alle bzgl. der Gleichverteilung unabhängigen Zufallsvariablen immer auf die Gestalt (1.2) bringen lassen, anwenden. In Kap. 3 folgern wir daraus sehr einfach, daß bzgl. $\frac{1}{n}$ 1 unabhängige, selbstadjungierte und kommutierende Matrizen immer unitär äquivalent sind zu Paaren der Gestalt $C\otimes 1$ und $1\otimes D$ (\otimes ...Tensor- oder Kronecker- oder direktes Produkt).

Ebenso betten sich alle weiteren klassischen Problemstellungen des ersten Abschnitts in den Gegenstand dieser Arbeit, der Bestimmung von k-tupeln von paarweise bzgl. $\frac{1}{n}$ 1 unabhängigen, selbstadjungierten, komplexen Matrizen: A_1, \ldots, A_k , als Spezialfall für kommutierende Matrizen ein. Dies erweist sich in vieler Hinsicht als natürliche Verallgemeinerung.

Die Dinge werden aber zugleich beträchtlich komplizierter. So führt bereits die Bestimmung einfacher Paare von bzgl. $\frac{1}{n}$ 1 unabhängigen, komplexen Matrizen auf ein schwieriges Problem.

13. EINE ANDERE FORMULIERUNG

Seien A und B beliebige selbstadjungierte, komplexe n×n Matrizen mit Spektralzerlegungen wie in der obigen Definition. Es sei eine feste orthonormierte Basis des \mathbb{C}^n gewählt, in der A eine geordnete Diagonalmatrix ist; das soll heißen: die Eigenwerte: a_1,\ldots,a_r (etwa in aufsteigender Reihenfolge geordnet) stehen nacheinander je mit Vielfachheit $k_i:=\operatorname{tr}(P_i)$ in der Diagonale. Dann ist P_i eine Diagonalmatrix mit zuerst k_i Einsen, dann Nullen in der Diagonale: $P_i=\operatorname{diag}(1,\ldots,1,0,\ldots,0)$; weiters hat $P_2=\operatorname{diag}(0,\ldots,0,1,\ldots,1,0,\ldots,0)$ zuerst k_i Nullen, dann k_i Einsen, dann Nullen, usw. Die Matrix B ist im allgemeinen nicht bereits auch diagonal. Sei U eine unitäre Matrix die B in eine geordnete Diagonalmatrix $\hat{B}=U^{-1}BU$ transformiert, d.h. analog sollen b_1,\ldots,b_n nacheinander mit Vielfachheit $b_i:=\operatorname{tr}(Q_i)$ die Diagonale von $b_i:=\operatorname{tr}(Q_i)$ die Diagonale von $b_i:=\operatorname{tr}(Q_i)$ diagonal: $b_i:=\operatorname{tr}(Q_i)$ die Diagonale von $b_i:=\operatorname{tr}(Q_i)$ diagonal: $b_i:=\operatorname{tr}(Q_i)$

$$U = \begin{bmatrix} U_{11} & U_{12} & \dots & U_{1s} \\ U_{21} & U_{22} & \dots & U_{2s} \\ \vdots & \vdots & & \vdots \\ U_{r1} & U_{r2} & \dots & U_{rs} \end{bmatrix}$$

d.h. so, daß die Matrizen: $\hat{\mathbf{U}}_{i,j} := P_i \mathbf{U} \, \hat{\mathbf{Q}}_j$ $1 \le i \le r$, $1 \le j \le n$ Jeweils nur noch die die Einträge der Submatrix $\mathbf{U}_{i,j}$ stehen haben, sonst nur Nullen.

Unter Verwendung von $P^2=P$ und $P^*=P$ (*=adjungiert) für orthogonale Projektionen und tr(MN)=tr(NM) für bel. Matrizen M und N folgt:

$$\operatorname{tr} \left(P_{_{\underline{i}}} Q_{_{\underline{j}}} \right) \ = \ \operatorname{tr} \left(P_{_{\underline{i}}} U \widehat{Q}_{_{\underline{j}}} U^{-1} \right) \ = \ \operatorname{tr} \left(P_{_{\underline{i}}} U \widehat{Q}_{_{\underline{j}}} \widehat{Q}_{_{\underline{j}}} U^{-1} P_{_{\underline{i}}} \right) \ = \ \operatorname{tr} \left(\widehat{U}_{_{\underline{i},\underline{j}}} \widehat{U}_{_{\underline{i},\underline{j}}}^{*} \right)$$

Mittels $\|C\|^2 := \operatorname{tr}(CC^*) = \sum |c_{ij}|^2$ wird die sogenannte Hilbert-Schmidt oder Euklidische Norm $\|C\|$ der Matrix $C = (c_{ij})$ definiert. Aus

$$\|\mathbf{\widetilde{U}}_{i,i}\|^2 = \|\mathbf{U}_{i,i}\|^2$$

und (1.4) folgt, daß A und B bzgl. $\frac{1}{n}$ 1 unabhängig sind, genau dann wenn: $\|\mathbf{U}_{i,i}\|^2 = \frac{1}{n}(k_i)_i \qquad \text{für alle } 1 \le i \le r, 1 \le j \le s$

1.2. **DEFINITION**: Eine komplexe $n \times n$ Matrix v heißt Verallgemeinerte Block Hadamard Matrix mit Partition:

$$\begin{aligned} k_{i}+k_{2}+\ldots+k_{r}&=n & l_{i}+l_{2}+\ldots+l_{s}&=n & k_{i},l_{j}\in\mathbb{N} \\ \text{abgekürzt VBH}(k_{i},\ldots,k_{r};l_{i},\ldots,l_{s})-\text{Matrix, falls:} \end{aligned}$$

- i) V ist unitär: VV^{*}=1
- ii) Bei Partition von $\mathbf{U}=(\mathbf{U}_{ij})$ in $\mathbf{k}_i \times \mathbf{l}_j$ Submatrizen \mathbf{U}_{ij} (wie oben) gilt: $\|\mathbf{U}_{ij}\|^2 = \frac{1}{n}(\mathbf{k}_i \mathbf{l}_j) \tag{1.5}$ für $1 \le i \le r$, $1 \le j \le s$.

Wir haben gezeigt, daß A und B unabhängig bzgl. $\frac{1}{n}$ 1 sind, genau dann, wenn ein wie oben zugeordnetes (nicht eindeutiges) U eine VBH-Matrix mit Partition $k_i = \mathbf{tr}(P_i)$, $l_j = \mathbf{tr}(Q_j)$ ist. Als Satz formulieren wir das in Kap.3, wo wir mittels Äquivalenzrelationen eine Eins zu Eins Zuordnung herstellen. Dies reduziert das Problem auf die Bestimmung der VBH-matrizen.

Wie bereits im Anschluß an Def.1.1. stellen wir fest, daß (1.5) nur (r-1)(s-1) unabhängige Bedingungen (für unitäre Matrizen) sind. Wir fordern wieder r≥2 und s≥2.

Man sieht unmittelbar, daß jede VBH-Matrix mit vorgegebener Partition auch eine solche mit gröberer Partition ist.

Beispiele mit nichttrivialer Blockzerlegung sind die VBH(2,2;2,2)-Matrizen:

$$\begin{bmatrix} \sin x & 0 & \cos x & 0 \\ 0 & \cos x & 0 & \sin x \\ \cos x & 0 & -\sin x & 0 \\ 0 & \sin x & 0 & -\cos x \end{bmatrix} \qquad x \in [0, 2\pi)$$

Wir nennen \mathbf{U} eine nichtentartete VBH-Matrix oder einfach VH-Matrix, falls $\mathbf{k_i} = \mathbf{l_j} = 1$ für $1 \le \mathbf{i}$, $\mathbf{j} \le \mathbf{n}$, das sind unitäre $\mathbf{n} \times \mathbf{n}$ Matrizen mit Einträgen $\mathbf{u_{ij}} \in \mathbb{C}$ sodaß: $|\mathbf{u_{ij}}|^2 = \frac{\mathbf{1}}{\mathbf{n}} \qquad \qquad \text{für alle } 1 \le \mathbf{i}$, $\mathbf{j} \le \mathbf{n}$

Zugeordnet sind unabhängige A und B mit nichtentartetem Spektrum.

1.4. HADAMARD-MATRIZEN UND IHRE VERALLGEMEINERUNGEN

Folgende Spezialfälle, vorerst von VH-Matrizen, sind wohlbekannt und Gegenstand einer Reihe von Untersuchungen:

- i) U sei eine VH-Matrix mit lauter reellen Einträgen. $H:=\sqrt{n}U$ hat dann Einträge $h_{ij}=\pm 1$ und erfüllt: $HH^T=n1$. Solche sogenannte Hadamard Matrizen H können nur für n=2 oder n=4t, $t\in \mathbb{N}$ existieren. Ihre Existenz wird für alle solchen n vermutet. Für einen Überblick bekannter Konstruktionen siehe Wallis [46], Agaian [02].
- ii) Komplexe Hadamard-Matrizen, $HH^*=n1$ mit Einträgen $h_{i,j}=\pm 1,\pm i$ wurden von Turyn eingeführt. Wie oben wird ihre Existenz für alle zulässigen Werte n=2t, $t \in \mathbb{N}$ vermutet. Daraus würde die Existenz gewöhnlicher Hadamard-Matrizen für n=4t, $t \in \mathbb{N}$ folgen. (Turyn [44])
- iii) Sei $\lambda = e^{2\pi i/n}$. Als n×n Fouriermatrix bezeichnen wir :

$$\mathbf{F}_{(n)} = \sqrt{\frac{1}{n}} \begin{bmatrix} \lambda^{(i-1)(j-1)} \\ \lambda^{(i-1)(j-1)} \end{bmatrix} = \sqrt{\frac{1}{n}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \lambda & \lambda^2 & & \lambda^{n-1} \\ 1 & \lambda^2 & \lambda^4 & & \lambda^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda^{n-1} & \lambda^{2(n-1)} & \dots & \lambda^{(n-1)(n-1)} \end{bmatrix}$$

 $F\infty$ ist unitär und ein Beispiel für eine VH-Matrix für alle n. (Siehe auch Auslander und Tolimieri [04]).

iv) Die vorhergehenden Punkte sind subsumiert unter der Definition verallgemeinerter Hadamard Matrizen, die auf Butson [12] zurückgeht: Mit $\mathbf{H}(k,n)$ bezeichnen wir n×n Matrizen mit Einträgen aus den k-ten Einheitswurzeln in \mathbb{C} , sodaß $\mathbf{HH}^*=\mathbf{n1}$. Gewöhnliche Hadamard-Matrizen sind $\mathbf{H}(2,n)$, komplexe $\mathbf{H}(4,n)$, \sqrt{n} $\mathbf{F}(n)$ sind $\mathbf{H}(n,n)$. Für eine Zusammenstellung weiterer bekannter Lösungen siehe Brock [09].

 \sqrt{n} H(k,n) lassen sich als (im Verhältnis zu 2Π) rationale Punkte auf den Lösungsmannigfaltigkeiten von VH-Matrizen interpretieren:

Beispiel:

$$U_{x} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{ix} & -1 & -e^{ix} \\ 1 & -1 & 1 & -1 \\ 1 & -e^{ix} & -1 & e^{ix} \end{bmatrix}$$

 $2 {\bf U_x}$ ist z.B. für x=0 eine gewöhnliche, für x= $\frac{\pi}{2}$ eine komplexe Hadamard-Matrix. ${\bf U_{\pi \times 2}}$ ist auch die Fouriermatrix.

Sogar jede 4×4 VH-Matrix ist zu einem $\mathbf{U}_{\mathbf{x}}$, für $\mathbf{x} \in [0,\frac{\pi}{2}]$ äquivalent. (Das heißt hier: Geht durch vertauschen von Zeilen bzw. Spalten und deren beliebige Multiplikation mit $\mathbf{x} \in \mathbb{C}$, $|\mathbf{x}| = 1$ daraus hervor.) Dasselbe gilt für die weiter oben angegebenen einparametr. Schar von VBH(2,2;2,2)-Matrizen mit einem allgemeinen Äquivalenzbegriff, der in Kapitel 3 definiert wird.

Allgemeine VBH-Matrizen, außer VH-Matrizen, wurden (soweit mir bekannt) in der Literatur noch nicht explizit untersucht. Es gibt aber einen Zusammenhang zu einer alternativen Definition von verallgemeinerten Hadamard Matrizen. Der Rest dieses Abschnitts soll ein Exkurs dazu sein (und kann, da ohne spätere Konsequenzen, auch übersprungen werden).

Eine verallgemeinerte n×n Hadamard Matrix $\mathbf H$ über einer endlichen Gruppe $\mathcal G$, $(GH(\mathcal G,n))$ ist definiert durch :

- i) Einträge h_{ij} sind Elemente von §
- ii) Die Menge (h_{ik}h_{jk} : 1≤k≤n) enthält für beliebige i≠j jedes Gruppenelement gleich oft.

Drake [21] nimmt die Forderung, daß mit ${\tt H}$ auch die transponierte Matrix ${\tt H}^{\tt T}$ diese Bedingungen erfüllt, in die Definition mit auf.

Eine andere Formulierung geht so: Sei $\mathbb{C}(\S)$ der Gruppenring von \S über \mathbb{C} . $\sum_{g \in \S} g$ erzeugt als Element von $\mathbb{C}(\S)$ ein Ideal I. Sei nun $\mathbb{R} = \mathbb{C}(\S)/I$. Interpretieren wir H als Matrix über \mathbb{R} und sei

$$H^* := (h_{ii}^{-1})$$

die transponierte Matrix mit invertierten Einträgen. ii) ist dann äquivalent zu: HH^{*}=□1 über R. Brock [09] verweist in diesem Zu-sammenhang kurz auf einen möglichen darstellungstheoretischen Hintergrund, den wir hier explizit anwenden.

Eine Darstellung $g \rightarrow U(g)$ von g in den komplexen $m \leftarrow m$ Matrizen sei gegeben, die:

- i) unitär ist: U*(g)=U⁻¹(g), ∀g∈ÿ
- ii) die triviale Darstellung (g → 1 ¥g) nicht enthält

Aus der $GH(\mathcal{G},n)$ Matrix $\mathbf{H}=(h_{i,j})$ bilden wir eine mn×mn Matrix über \mathbb{C} :

$$\mathbf{U}(\mathbf{H}) := \sqrt[4]{\mathbf{U}(h_{11})} \quad \mathbf{U}(h_{12}) \quad \dots \quad \mathbf{U}(h_{1n}) \\ \vdots & \vdots & \vdots \\ \mathbf{U}(h_{n1}) \quad \mathbf{U}(h_{n2}) \quad \dots \quad \mathbf{U}(h_{nn}) \end{bmatrix}$$

U(H) ist dann eine VBH-Matrix, mit Partition k_i=l_j=m, ±≤i.j≤n, wie sich leicht sehen läβt:

Aus der Unitarität der Darstellung folgt:

$$U^*(H) = U(H^*)$$

Nach dem Satz von Maschke zerfällt jede Darstellung einer (endl.) Gruppe $\mathcal G$ in eine direkte Summe irreduzibler Darstellungen, wobei aus deren Orthogonalitätsrelationen (siehe Curtis/Reiner [15],§31) folgt, daß, falls $g \to \mathbf U(g)$ die triviale Darstellung nicht enthält, gilt: $\sum_{g \in \mathcal G} \mathbf U(g) = 0$.

Zusammen ergibt dies die Unitarität von $\mathbf{U}(\mathbf{H})$: $\mathbf{U}(\mathbf{H})\mathbf{U}^*(\mathbf{H})=1$ Ebenso folgt leicht:

$$\operatorname{tr}\left(\frac{1}{n}U(h_{ij})U^{*}(h_{ij})\right) = \frac{1}{n}\operatorname{tr}(1_{m}) = \frac{m}{n} = \frac{1}{mn}(k_{i})_{j},$$

Dies liefert also Einbettungen der $GH(\mathcal{G},n)$ – in die VBH-Matrizen. Bislang wurden vor allem $GH(\mathcal{G},n)$ -Matrizen mit elementaren abelschen Gruppen: $\mathcal{G} = EA(p^m) \cong (\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p, +)$ untersucht. (Seberry [39], Dawson [17], de Launey [18]). Deren treue, unitäre Darstellung durch die m×m Matrizen:

$$\left[\begin{array}{ccc} e^{2\pi i\lambda(\mathbf{1})/p} & & & \\ & \cdot & & \\ & & \cdot & \\ & & e^{2\pi i\lambda(m)/p} \end{array}\right] \quad \lambda(\mathbf{j}) \in \{\mathbf{0},\dots,p-\mathbf{1}\}, \ \mathbf{1} \leq \mathbf{j} \leq \mathbf{m}$$

gibt dann eine solche Standard-Einbettung an. Erst kürzlich gelang de Launey [19] erstmals eine Konstruktion von GH(\$\mathbf{G},n)-Matrizen für nicht elementar abelsche Gruppen \$\mathbf{G}.

15. PRODUKTE VON VBH-MATRIZEN

A,B und C seien komplexe, selbstadj. n×n Matrizen, die paarweise bzgl. $\frac{1}{n}$ 1 unabhängig sind. A liege in geordneter Diagonalform vor. Die Unabhängigkeit bzgl. $\frac{1}{n}$ 1 von A und B bzw. A und C kann durch zwei unitäre Matrizen U und V beschrieben werden, die $B \rightarrow U^{-1}BU$, bzw. $C \rightarrow V^{-1}CV$ jeweils in geordnete Diagonalform transformieren. U und V müssen VBH-Matrizen sein, entsprechend der Blocknotation:

$$\mathbf{U} = \begin{bmatrix} \mathbf{U}_{.\mathbf{ii}} & ... & \mathbf{U}_{.\mathbf{s}} \\ \vdots & \vdots & \vdots \\ \mathbf{U}_{r\mathbf{i}} & ... & \mathbf{U}_{r\mathbf{s}} \end{bmatrix} \qquad \text{bzw.} \qquad \mathbf{V} = \begin{bmatrix} \mathbf{V}_{.\mathbf{ii}} & ... & \mathbf{V}_{.\mathbf{it}} \\ \vdots & \vdots & \vdots \\ \mathbf{V}_{r\mathbf{i}} & ... & \mathbf{V}_{r\mathbf{t}} \end{bmatrix}$$

Mit $k_i \times l_j$ Submatrizen \mathbf{V}_{ij} , $1 \le i \le r$, $1 \le j \le s$, bzw. $k_i \times m_j$ Submatrizen \mathbf{V}_{ij} , $1 \le i \le r$, $1 \le j \le t$. Wobei k_i , l_i bzw. m_i jeweils die Dimensionen der Eigenräume sind, die zum i-ten Eigenwert von A, B bzw. C gehören.

Wie läßt sich nun die Unabhängigkeit bzgl. $\frac{1}{n}$ 1 von B und C durch U und V charakterisieren? Wir transformieren das Paar B, C in eine Basis in der B in geordn. Diagonalform ist, z.B. durch $B \rightarrow U^{-1}BU$ und $C \rightarrow U^{-1}CU$ und suchen ein unitäres W, welches $U^{-1}CU$ in geordnete Diagonalform transformiert. Eine Lösung ist $W = U^{-1}V$, da

$$V^{-1}CV = W^{-1}(U^{-1}CU)W$$

Also muß auch $W=U^{-1}V$ eine VBH-Matrix sein und zwar mit $l_i \times m_j$ Submatrizen $W_{i,j}$, $1 \le i \le s$, $1 \le j \le t$:

$$U^{-1}V = W = \begin{bmatrix} W_{11} \dots W_{11} \\ \vdots & \vdots \\ W_{s1} \dots W_{st} \end{bmatrix}$$

Dieses Produkt ist mit den Partitionen der Matrizen verträglich, d.h. es läβt sich in Blocknotation schreiben:

$$W_{i,j} = \sum_{k=1}^{r} U_{ki}^{*} V_{kj}$$

 $W = U^{-1}V \Leftrightarrow V = U.W$. Wir können das Problem auch so formulieren: Untersuche Produkte von VBH-Matrizen mit verträglicher Partition, (d.h. das Produkt soll sich in Blocknotation schreiben lassen können), inwiefern sie selbst wieder VBH-Matrizen (mit der natürlich resultierenden Partition) bilden. Oder: Suche Zerlegungen von VBH-Matrizen in Produkte zweier verträglicher VBH-Matrizen.

VBH-Matrizen mit trivialer Partition (d.h. wo sich Blöcke über ganze Zeilen oder Spalten erstrecken) sind genau die unitären Matrizen. Diese bilden eine Gruppe. Verfeinerung der Partition bedeutet Einschränkung der Lösungen auf Teilmengen, jener von gröberer Partition. Insbesondere untersuchen wir also, was von der ursprünglich allgemein wohldefinierten Verknüpfung unitärer Matrizen bei diesen Einschränkungen jeweils noch übrigbleibt.

Wir geben ein Beispiel aus VH-Matrizen an. Für x,y,z ∈ [0,2π) sei:

$$\mathbf{V}_{x} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{ix} & -1 & -e^{ix} \\ 1 & -1 & 1 & -1 \\ 1 & -e^{ix} & -1 & e^{ix} \end{bmatrix} \qquad \mathbf{V}_{yz} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ e^{iy} & e^{iz} - e^{iy} - e^{iz} \\ 1 & -1 & 1 & -1 \\ -e^{iy} & e^{iz} & e^{iy} - e^{iz} \end{bmatrix}$$

Mit $\mathbf{U}_{\mathbf{x}}^{-1} = \mathbf{U}_{\mathbf{x}}^{*} = \mathbf{U}_{-\mathbf{x}}$ folgt leicht:

$$\mathbf{U}_{x}^{-1}\mathbf{V}_{yz} = \frac{1}{2} \begin{bmatrix} 1 & e^{iz} & 1 & -e^{iz} \\ e^{iv} & 1 & -e^{iv} & 1 \\ 1 & -e^{iz} & 1 & e^{iz} \\ -e^{iv} & 1 & e^{iv} & 1 \end{bmatrix} \quad \text{mit } w=y-x$$

 $\mathbf{v}_{\mathbf{x}}$, $\mathbf{v}_{\mathbf{yz}}$ und $\mathbf{v}_{\mathbf{x}}^{-1}\mathbf{v}_{\mathbf{yz}}$ sind für bel. $\mathbf{x},\mathbf{y},\mathbf{z}\in[0,2\pi)$ 4×4 VH-Matrizen. (Die letzteren beiden sind äquivalent zu den $\mathbf{v}_{\mathbf{x}}$, siehe oben). Zugeordnet sind Tripel paarweise bzgl. $\frac{1}{4}$ 1 unabhängiger, selbstadjungierter, nichtentarteter 4×4 Matrizen. Bezogen auf den allgemeinen Äquivalenzbegriff, den wir in Kap. 3 definieren werden, sind dies bereits alle entsprechenden Lösungen.

Die Erweiterung von Tripel auf k-tupel, paarweise bzgl. $\frac{1}{n}$ 1 unabhängiger n×n Matrizen A_1, \ldots, A_k ist offensichtlich. Zugeordnet sind k-1 unitäre n×n Matrizen U_1, \ldots, U_{k-1} . Die U_i müssen VBH-Matrizen mit Partitionen, entsprechen den Eigenraumdimensionen von A_1 und A_{i+1} , sein. Ebenso müssen alle $U_i^{-1}U_j$ für $i \not= j$ VBH-Matrizen mit Partitionen entsprechend den Eigenraumdimensionen von A_{i+1} und A_{j+1} sein. (Es genügt für $i \not= j$ zu zeigen).

Wir nennen die $\mathbf{U_i}, \dots, \mathbf{U_{k-i}}$ dann kurz k-1 "VBH-Matrizen mit Produkt-eigenschaft".

1.6. KURZER ÜBERBLICK

Im nächsten, zweiten Kapitel wird Def.1.1 aus der wahrscheinlichkeitstheoretischen Interpretation des Hilbertraumformalismus abgeleitet und diskutiert. Es werden auch Beispiele in unendlichdimensionalen Räumen angegeben. Kapitel 2 kann auch übersprungen werden.
Es bettet das bisher Behandelte in einen breiteren Kontext ein. Für
die in Kap. 3 bis 5 sich anschließende detailiertere Untersuchung
der in der Einleitung skizzierten Problemstellung ist das aber
nicht notwendig.

In Kapitel 3 werden vorerst (technische) Äquivalenzbegriffe definiert. Eine auch sonst nützliche geometrische Interpretation liefert sofort eine Ungleichung, welche die klassische Formel (1.3) verallgemeinert. Grundlegende Eigenschaften des Tensorprodukts werden in der Folge immer wieder verwendet.

Kapitel 4 enthält die Hauptkonstruktion dieser Arbeit. Sei n=q¹, mit einer beliebigen Primzahlpotenz q und bel. L∈N. Wir zeigen die Existenz von (q²¹-1)/(q-1) selbstadjungierten n×n Matrizen die paarweise unabhängig bzgl. ½1 sind, wobei jede dieser Matrizen genau q verschiedene Eigenwerte mit jeweiliger Eigenraumdimension q¹⁻¹ hat. Für L=1 sind das q+1 nichtentartete q×q Matrizen. Diese Lösungen sind alle vollständig, d.h. die Anzahl der Matrizen ist im Sinne der Ungleichungen von Kapitel 3 maximal.

Der hierbei verwendete Ansatz hat ein Gegenstück im Unendlichdimensionalen (siehe Abschnitt 2.3). Bekannte Konstruktionen vollständiger Mengen paarweise orthog. Lateinischer Quadrate, bzw. Orthog. Anordnungen sind als Teillösungen enthalten.

Für ungerade Primzahlpotenzen erhält man das Resultat auch kürzer über eine explizite Formel für 9 VH-Matrizen der Ordnung 9 mit Produkteigenschaft. Für Zweierpotenzen ist eine solche Formel noch nicht bekannt.

Kapitel 5 versammelt einige Untersuchungen zu VBH-Matrizen und Konstruktionen von VH-Matrizen. Im dritten Abschnitt wird ein spezielles Produkt von VH-Matrizen analysiert. Die Anwendung dieser Ergebnisse und Suchprogramme auf einem Personalcomputer führten alle nicht zur Auffindung von drei 6×6 VH-Matrizen mit Produkteigenschaft. Dies bedeutet, daß es wahrscheinlich keine vier selbstadjungierten 6×6 Matrizen mit jeweils 6 verschiedenen Eigenwerten (nichtentartet) gibt, die paarweise bzgl. $\frac{1}{6}$ 1 unabhängig sind. Das berühmte Resultat der Nichtexistenz zweier orthogonaler Lateinischer 6×6 Quadrate ist, nach den Ausführungen in Abschnitt 1.1 und eingebettet in die verallgemeinerte Theorie, äquivalent dazu, daß es keine vier selbstadjungierten, kommutierenden 36×36 Matrizen mit jeweils 6 verschieden Eigenwerten gibt, die paarweise bzgl. $\frac{1}{36}$ 1 unabhängig sind.

Diese zeigte eine enge Analogie zwischen kommutativem und nichtkommutativem Fall. In beiden Fällen würden vollständige solche Lösungen, wie sie für alle Primzahlpotenzordnungen in Kapitel 4 konstruiert werden, 7 derartige Matrizen umfassen.

Kapitel 6 behandelt zuletzt Anwendungen in der Quantenmechanik. Wir diskutieren vor allem das Problem der sogenannten Informationsvollständigkeit. Die vollständigen Lösungen aus Kap.4 liefern hierbei Gegenbeispiele zu einer Vermutung von Moroz [34]. Eine kurze Bemerkung über die prinzipielle Bedeutung der Begriffsbildung für die Quantenmechanik schließt die Arbeit.

2.UNABHÄNGIGKEIT

Vorkenntnisse aus der Quantenmechanik werden nicht vorausgesetzt. Das Konzept der verallgemeinerten, nichtkommutativen Wahrscheinlichkeitstheorie, das dieser zugrundeliegt, wird in Absschnitt 2.1 zusammengefaßt. In Abschnitt 2.2 werden verschiedene Interpretationen von Def.1.1 und ihr Verhältnis zur allgemeinen Definition von Unabhängigkeit im \mathbb{C}^n behandelt. Im letzten Abschnitt wird die Problematik in unendlichdimensionalen Hilberträumen behandelt.

2.1. GRUNDLAGEN

Unsere Notation folgt vor allem Reed/Simon [37]

೫ sei ein komplexer, separabler Hilbertraum.

Pe $\mathcal P$ seien die orthogonalen Projektionsoperatoren auf die (abgeschlossenen) Unterräume von $\mathcal R$. Es gilt: $\mathbf P^2=\mathbf P$, sowie $\mathbf P^*=\mathbf P$. Hat der Teilraum endliche Dimension k, existiert die Spur und ist: $\mathrm{tr}(\mathbf P)=k$. Die $\mathbf P\in\mathcal P$ korrespondieren zu Eigenschaften (Ereignissen) eines quantenmechanischen Systems. Sie bilden den Ersatz für die Ereignis- σ -Algebra Σ der klassischen Wahrscheinlichkeitstheorie.

Dichteoperatoren D∈D sind:

- i) selbstadjungiert: D*=D
- ii) postiv semidefinit: <x,Dx> ≥ Ø, ∀x∈%
- iii) normiert: tr(D)=1

D∈⊅ beschreiben Zustände (Präparationen) des Systems. Sie definieren Wahrscheinlichkeitsmaße auf ⊅:

Um die Eigenschaften bzw. Zustände des Systems zu bezeichnen verwenden wir im folgenden jeweils ebenfalls die Symbole der zugeordneten Operatoren. Wir sprechen also von der Wahrscheinlichkeit von P bei Vorliegen von D. Diese ist definiert durch:

$$\mu_{\mathbf{p}}(\mathbf{P}) := \mathsf{tr}(\mathbf{PD})$$

 $\mu_{\mathbf{p}}$ ist ein Maß auf $\mathcal P$ mit folgenden Eigenschaften:

i) μ_p : 𝒫 → [0,1]

(2.1)

 $\begin{array}{ll} \text{ii)} & \mu_{_{\mathbf{D}}}(\mathbf{1}) = \mathbf{1}_{_{\mathbf{D}}} \\ \text{iii)} & \mu_{_{\mathbf{D}}}(\mathbf{P}) = \sum\limits_{i = 1}^{n} \mu_{_{\mathbf{D}}}(\mathbf{P}_{_{i}}) \text{, falls } \mathbf{P} = \text{s-lim} \Big(\sum\limits_{n \to \infty}^{n} \mathbf{P}_{_{i}} \Big) & \text{(starke Konvergenz)} \\ & \text{starke Konvergenz)} \\ & \text{starke Konvergenz)} \end{array}$ und die $\mathbf{P_i}$ paarweise orthogonale Proj. sind $(\mathbf{P_iP_j}\text{=}\emptyset\text{, für }\text{i}\text{\neq}\text{j})\text{.}$

Nach einem bekannten Satz von Gleason [23] gibt es für Jedes Maß μ über %, dim(%)≥3, welches i)→iii) erfüllt, einen eindeutigen Dichteoperator D, sodaß $\mu=\mu$.

Zufallsvariablen korrespondieren zu selbstadjungierten Operatoren A (in der Quantenmechanik Observablen genannt). Sei $z_{\mathbf{p}}$ die charakteristische Funktion einer Borelmenge BSR, $\chi_{_{\rm B}}({\bf A})$ \in ${\mathcal P}$ ist ein Spektralprojektor von A. (Dies entspricht $f^{-1}(B) \in \Sigma$ für klassische Zufallsvariablen). $\mu_{\mathbf{D}}(\chi_{\mathbf{p}}(\mathbf{A})) = \text{tr}(\mathbf{D}.\chi_{\mathbf{p}}(\mathbf{A}))$

gibt die Wahrscheinlichkeit an bei Vorliegen von D einen Wert für A in B⊆R zu messen.

Die so definierte quantenmechanische Wahrscheinlichkeitstheorie umfaßt die klassische Kolmogorov'sche als Spezialfall. Eine Einbettung gibt z.B. Gudder [25], p.53 an; klassische Zufallsvariablen werden hierbei auf kommutierende Operatoren abgebildet.

Wir notieren noch wichtige Eigenschaften der Spur (Reed/Simon [37], Theorem VI 19,24,25):

- i) tr(A) ist auf der sogenannten Spurklasse $\mathcal{P}_{-}=\{A: beschr., tr|A|\leq \infty\}$ wohldefiniert, d.h. von der Basis unabhängig ($|A|=(A^*A)^{1/2}$).
- ii) $\mathcal{P}_{\mathbf{i}}$ ist ein Ideal in $\mathcal{Z}(\mathcal{R})$, den beschränkten Operatoren. (2.2)iii) $\mathcal{D} \subseteq \mathcal{P}_{\downarrow}$
 - iv) tr(A+B)=tr(A)+tr(B), $tr(\lambda A)=\lambda tr(A)$
 - v) $\operatorname{tr}(\mathbf{A}\mathbf{B}) = \operatorname{tr}(\mathbf{B}\mathbf{A})$, falls $\mathbf{A} \in \mathcal{P}_{\mathbf{i}}$ und $\mathbf{B} \in \mathcal{E}(\mathcal{R})$

Erwähnt werden sollen noch einige Eigenschaften orthogonaler Projektionen auf eindimensionale Teilräume. Sie lassen sich explizit angeben. Sei in einer orthonormierten Basis von \mathscr{R} : $e = (e_i)_{i=1}^{\infty}$ ein normierter Vektor (∥e∥=1). Den in dieser Basis durch die Matrix $(e_i^*)_{i,j=1}^\infty$ beschriebenen Operator bezeichnen wir mit P_e . Er ist

die orthogonale Projektion auf den durch ⊜ aufgespannten eindim. Teilraum. Es folgen leicht die Formeln:

i)
$$\operatorname{tr}(P_{e}A) = \langle e | Ae \rangle \qquad \operatorname{tr}(P_{e}P_{f}) = \left| \langle e | f \rangle \right|^{2}$$
ii)
$$P_{e}AP_{e} = \langle e | Ae \rangle P_{e} \qquad P_{e}P_{f}P_{e} = \left| \langle e | f \rangle \right|^{2}P_{e} \qquad (2.3)$$

Ist der Dichteoperator $\mathbf{D}=\mathbf{P}_{\mathbf{e}}$ so spricht man von reinen Zuständen. Die Wahrscheinlichkeit einer durch $\mathbf{P}_{\mathbf{f}}$ beschriebenen Eigenschaft ist dann $|\langle \mathbf{e} | \mathbf{f} \rangle|^2$. Dieser Ausdruck wird auch oft als Ausgangspunkt für Darstellungen der Quantenmechanik genommen.

Um jetzt zu einer Definition der Unabhängigkeit von Eigenschaften (bzw. Observablen) zu gelangen, überlegen wir uns, wie zwei Eigenschaften P,Q des Systems eine gemeinsame Wahrscheinlichkeit bzgl. D zugeordnet werden kann. Es gibt zwei Möglichkeiten:

- i) Die auf John v. Neumann und G. Birkhoff zurückgehende quantenlogische Interpretation der Quantenmechanik nimmt die Verbandsstruktur der abgeschlossenen Unterräume von % als vollwertigen Ersatz für die klassische σ -Algebra Σ . Es liegt also nahe einen Operator $\mathbf{P} \sim \mathbf{Q}$ als Projektor auf jenen Teilraum von % zu definieren, der als Durchschnitt der zu \mathbf{P} und \mathbf{Q} gehörigen Teilräume ensteht $(\mathbf{P} \sim \mathbf{Q} = \mathbf{S} \mathbf{l} \cdot \mathbf{j}_{\mathbf{Q}} (\mathbf{P} \mathbf{Q})^n)$. Erst kürzlich wurden die Eigenschaften der gemeinsamen Wahrscheinlichkeit $\mu_{\mathbf{p}} (\mathbf{P} \sim \mathbf{Q})$ in einem Buch von Pitowsky [35] ausführlich untersucht. Unabhängig bzgl. \mathbf{P} heißen folgerichtig \mathbf{P} und \mathbf{Q} falls $\mu_{\mathbf{p}} (\mathbf{P} \sim \mathbf{Q}) = \mu_{\mathbf{p}} (\mathbf{P}) \cdot \mu_{\mathbf{p}} (\mathbf{Q})$ (siehe Gudder [24], chap.2.2).
- ii) Für den zweiten Ansatz, den wir uns zu eigen machen, suchen wir vorerst einen Ausdruck für die bedingte Wahrscheinlichkeit $\mu_{_{\rm D}}({\rm P/Q})$ analog zur klassischen Wahrscheinlichkeitstheorie: Wir fordern:
- i) $P \rightarrow \mu_{_{\mathbf{D}}}(P/Q)$ ist ein Wahrscheinlichkeitsmaß auf \mathcal{P} (entsprechend den Gleichungen (2.1)) für alle D und Q, für die $\mu_{_{\mathbf{D}}}(Q) \neq \emptyset$ gilt. ii) $\mu_{_{\mathbf{D}}}(P/Q) = \mu_{_{\mathbf{D}}}(P)/\mu_{_{\mathbf{D}}}(Q)$ für $P \leq Q$ (d.h. QP = P)

Beltrametti und Cassinelli ([06], chap. 26.2) zeigen mithilfe des Satzes von Gleason, daß daraus folgt:

$$\mu_{\mathbf{D}}(P/Q) = \frac{\text{tr}(PQDQ)}{\text{tr}(QD)}$$
 (2.4)

(siehe auch Gudder [25] Th.5.26). Verschiedentlich wurde bemerkt,

daß diese Formel äquivalent ist zur Beschreibung der Zustandsänderung durch Messung nach Lüders [32] (siehe auch die Diskussion in Bub [10]):

Der Zustand des Systems sei durch den Dichteoperator D beschrieben. Q sei eine orthogonale Projektion. Die Messung von Q verändert D:

$$D \rightarrow D' = \frac{QDQ}{tr(QD)}$$
 (2.5)

wobei die Wahrscheinlichkeit von Q ungleich Null, d.h:

$$\mu_{\mathbf{D}}(\mathbf{Q}) = \mathsf{tr}(\mathbf{Q}\mathbf{D}) \neq \emptyset$$

vorausgesetzt wurde. D'ist, wie leicht nachzuprüfen, ein Dichte-operator. (Falls z.B. $Q=P_{\underline{a}}$ ist, so folgt mit (2.3) $D \to P_{\underline{a}}$). Messen wir jetzt anschließend P, so ist dessen Wahrscheinlichkeit (bei bestätigtem Q, d.h. in dem nun vorliegenden Zustand D'):

$$\mu_{_{\mathbf{D}}}$$
, $(P) = \text{tr}(PD') = \frac{\text{tr}(PQDQ)}{\text{tr}(QD)} = \mu_{_{\mathbf{D}}}(P/Q)$

Unter Entlehnung des "sequentiellen und": □ aus der Notation von von Mittelstaedt [33] definieren wir nun:

$$\mu_{_{\mathbf{D}}}(\mathbf{Q} \cap \mathbf{P}) := \mu_{_{\mathbf{D}}}(\mathbf{P}/\mathbf{Q}) , \mu_{_{\mathbf{D}}}(\mathbf{Q})$$
 d.h. mit (2.4):
$$\mu_{_{\mathbf{D}}}(\mathbf{Q} \cap \mathbf{P}) = \mathrm{tr}(\mathbf{P} \mathbf{Q} \mathbf{D} \mathbf{Q}) = \mathrm{tr}(\mathbf{Q} \mathbf{P} \mathbf{Q} \mathbf{D})$$
 (2.6)

Dies entspricht der Definition der gemeinsamen Wahrscheinlichkeit in der klass. Wahrscheinlichkeitstheorie. Offensichtlich ist aber i.A.: $\mu_{\mathbf{D}}(\mathbf{P} \cap \mathbf{Q}) \neq \mu_{\mathbf{D}}(\mathbf{Q} \cap \mathbf{P})$, d.h. diese Wahrscheinlichkeit hängt im Gegensatz zur klass. Theorie von der Reihenfolge ab.

Mit obiger Beschreibung der Zustandsänderung durch Messung läßt sich $\mu_{\mathbf{D}}(\mathbf{Q} \cap \mathbf{P})$ ein praktischer Messvorgang zuordnen, d.h. operativ interpretieren: Das ist genau die Wahrscheinlichkeit bei Messung von zuerst \mathbf{Q} und dann \mathbf{P} jeweils ein positives Ergebnis zu erhalten.

Die folgende Definition der Unabhängigkeit von P und Q ergibt sich nun ebenfalls völlig analog zur klass. Wahrscheinlichkeitstheorie, wobei aber auch die Unabhängigkeit der Wahrscheinlichkeit von der Reihenfolge der Messungen gelten soll, also:

$$\mu_{_{\mathbf{D}}}(\mathsf{P} \sqcap \mathsf{Q}) = \mu_{_{\mathbf{D}}}(\mathsf{Q} \sqcap \mathsf{P}) = \mu_{_{\mathbf{D}}}(\mathsf{P}) \cdot \mu_{_{\mathbf{D}}}(\mathsf{Q})$$

(2.6) eingesetzt gibt:

2.1. **DEFINITION**: Zwei orthogonale Projektionsoperatoren P und Q heißen unabhängig bezüglich dem Dichteoperator D, falls gilt: tr(PQPD) = tr(QPQD) = tr(PD).tr(QD) (2.7)

Die Iteration des Messprozeßes (2.5) und der bedingten Wahrscheinlichkeit (2.4) diskutiert z.B. Srinivas [41]. Damit läßt sich dann Unabhängigkeit für drei, vier und mehr Projektionen definieren. Wir beschränken uns aber ausschließlich auf paarweise Unabhängigkeit.

2.2. BEISPIEL: Kommutieren P und Q, so ist der erste Teil der Gleichung (2.7) für alle D erfüllt: Unter Verwendung von (2.2) ist: tr(PQPD) = tr(QPQD)

Der zweite Teil entspricht einer klassischen Formel: Wir wählen eine orthonormierte Basis $(\mathbf{e}_i)_{i=1}^\infty$ von $\mathscr R$, aus gemeinsamen Eigenvektoren \mathbf{e}_i von \mathbf{P} und \mathbf{Q} . \mathbf{I} , $\mathbf{J} \subseteq \mathbb{N}$ seien nun jene Indexmengen, sodaß gilt: $\mathbf{P} \mathbf{e}_i = \mathbf{e}_i$ für $\mathbf{I} \mathbf{e} \mathbf{I}$, $\mathbf{P} \mathbf{e}_i = \mathbf{e}_i$ für $\mathbf{I} \mathbf{e} \mathbf{I}$, $\mathbf{Q} \mathbf{e}_i = \mathbf{e}_i$ für $\mathbf{I} \mathbf{e} \mathbf{I}$. Sei

$$\nu\omega := \langle e_i | De_i \rangle \ge \emptyset \quad \forall i \in \mathbb{N} \quad \Rightarrow \quad \sum_{i=1}^{\infty} \nu\omega = \text{tr}(D) = 1$$

ν ist ein Wahrscheinlichkeitsmaß über Ν. Es folgt sofort:

$$\nu(\mathbf{I}) = \text{tr}(PD)$$
 $\nu(\mathbf{J}) = \text{tr}(QD)$ $\nu(\mathbf{I}\cap\mathbf{J}) = \text{tr}(PQD)$
Globa. (2.7) ist also äquivalent zu: $\nu(\mathbf{I}\cap\mathbf{J}) = \nu(\mathbf{I}) \cdot \nu(\mathbf{J})$

Auf einen weiteren wichtigen Spezialfall verweist folgendes Lemma:

2.3. LEMMA: A sei ein beschränkter, selbstadjungierter Operator, P_e , P_f orthogonale Projektionen auf eindimensionale Teilräume: aus $\operatorname{tr}(P_eP_fP_eA) = \operatorname{tr}(P_fP_eP_fA)$ für beliebige P_e und $P_f \Rightarrow A = \lambda 1$, $\lambda \in \mathbb{R}$.

Bew.: Unter Verwendung von (2.3.ii):

$$|\langle e|f\rangle|^2 tr(P_A) = |\langle e|f\rangle|^2 tr(P_A)$$

also vorerst für |⟨e|f⟩|²≠0 gilt:

$$tr(P_A) = tr(P_A)$$
.

Durch Zwischenschalten eines P_g , mit $\langle e | g \rangle \neq \emptyset$ und $\langle f | g \rangle \neq \emptyset$ folgt: $tr(P_A) = \langle e | Ae \rangle = \lambda \qquad \qquad \text{für alle } e \in \mathcal{H}, \ \|e\| = 1.$

 $\lambda \in \mathbb{R}$, da A selbstadjungiert ist und für das selbstadjungierte A- $\lambda 1$: $\langle e \mid (A-\lambda 1)e \rangle = \emptyset$ für alle $e \in \mathcal{H}$

Daraus folgt (siehe z.B.: Hirzebruch/Scharlau [28], Kor.22.5):

$$A-\lambda 1 = \emptyset$$

Das heißt: soll der erste Teil von (2.7) für alle orthogonalen Projektionen auf eindimensionale Teilräume erfüllt sein, muß D=λ1 sein. Nur in endlichdim. Hilberträumen kann dies ein (normierter) Dichteoperator sein. Setzen wir im \mathbb{C}^n : $D=\frac{1}{n}1$. Es gilt:

$$\frac{1}{p}$$
tr (PQP) = $\frac{1}{p}$ tr (PQ) = $\frac{1}{p}$ tr (QPQ)

Der erste Teil von (2.7) ist damit für bel. orthog. Proj. erfüllt. Der Dichteoperator $\frac{1}{n}$ 1 beschreibt den Zustand völliger Unkenntnis und ist sozusagen auf ganz 90 "homogen".

2.2. UNABHÄNGIGKEIT IM C" :

Behandeln wir vorerst $D = \frac{1}{n}1$: Mit dem zweiten Teil von (2.7) folgt: Zwei orthogonale Projektionen P und Q im Cⁿ sind unabhängig bzgl. 11 falls: $tr(PQ) = \frac{i}{p} tr(P), tr(Q)$

In der Einleitung definierten wir bereits die Unabhängigkeit bzgl. ¹¹¹ von selbstadj. Matrizen (Def.1.1); Sei deren Spektralzerlegung:

$$A = \sum_{i=1}^{r} a_i P_i \quad \text{und} \quad B = \sum_{j=1}^{m} b_j Q_j$$

 $\mathbf{A} = \sum_{i=1}^r a_i P_i \quad \text{und} \quad \mathbf{B} = \sum_{j=1}^n b_j Q_j$ $a_i \text{, } b_j \text{ die Je verschiedenen Eigenwerte, } P_i \text{,} Q_j \text{ die assozierten Pro-}$ jektionen auf die Eigenräume. (Wir halten an dieser Notation im ganzen Abschnitt fest). Sie sind unabhängig bezüglich $\frac{1}{n}$ 1, falls:

$$\operatorname{tr}(P_i^{}Q_j^{}) \; = \; \tfrac{\mathfrak{s}}{n} \; \operatorname{tr}(P_i^{}) \; . \\ \operatorname{tr}(Q_j^{}) \qquad \text{für alle } \mathfrak{s} \leq i \leq r \; , \; \mathfrak{s} \leq j \leq s \; .$$

Das heißt alle Paare P_i , Q_i müssen unabhängig bzgl. $\frac{1}{n}$ 1 sein.

In der quantenmechan. Literatur, wurde bislang nur ein Spezialfall davon behandelt. Sind A und B nichtentartet, d.h. P_i und Q_j Proj. auf eindim. Teilräume, so schreibt sich diese Forderung als:

$$\operatorname{tr}(P_iQ_j) = \frac{1}{n}$$
 für alle 1≤i,j≤n

Julian Schwinger [38] bezeichnete diese Gleichung als Ausdruck eines "maximum degree of incompatibility" und die Observablen A und B dann als "komplementär". Er stieß darauf bei der Untersuchung des diskreten Analogons der kanon. Vertauschungsrelationen. Accardi [O1] stellte im Anschluß daran als Problem (I.f) seiner Arbeit die Aufgabe der Bestimmung und Klassifikation aller Lösungen .

- 2.4. Proposition: Sind A und B unabhängig bzgl. $D=\frac{1}{D}$, so folgt:
 - i) $P:=\sum_{i\in I}P_i$ und $Q:=\sum_{j\in J}Q_j$ mit beliebigen Indexmengen $I\subseteq\{1,2,\ldots,r\}$, $J\subseteq\{1,2,\ldots,s\}$ sind unabhängig bzgl. $\frac{1}{r}1$.
- ii) Mit beliebigen Funktionen f,g: $\mathbb{R} \to \mathbb{R}$ sind f(A) und g(B) unabhängig bzgl. $\frac{1}{n}$ 1.

$$\mathsf{Bew.:} \quad \mathsf{i)} \quad \mathsf{tr}(\mathsf{PQ}) \ = \sum_{\mathsf{i} \ \in \mathbf{I}} \sum_{\mathsf{j} \ \in \mathbf{J}} \mathsf{tr}(\mathsf{P}_{\mathsf{i}}\mathsf{Q}_{\mathsf{j}}) \ = \sum_{\mathsf{i} \ \in \mathbf{I}} \sum_{\mathsf{j} \in \mathbf{J}} \mathsf{tr}(\mathsf{P}_{\mathsf{i}}) \, \mathsf{tr}(\mathsf{Q}_{\mathsf{j}}) \ = \ \mathsf{tr}(\mathsf{P}) \, \mathsf{tr}(\mathsf{Q})$$

ii) folgt aus i), da Eigenprojektionen von $f(A) = \sum_{i=1}^{r} f(a_i)P_i$ von der Gestalt $\sum_{i \in I} P_i$ sind, analog für g(B).

Das entspricht völlig der klassischen Wahrscheinlichkeitstheorie. Dort folgt für diskrete Zufallsvariable aus der Unabhängigkeit der Urbilder jedes der (singulären) Werte die Unabhängigkeit der Urbilder jeder beliebigen Wertemenge.

Prop. 2.4 gilt aber nicht für beliebige **D**. Das zwingt uns in der folgenden Definition der Unabhängigkeit selbstadjungierter Matrizen bzgl. beliebigen **D** zu einer Aufspaltung:

- i) schwach unabhängig bzgl. D, falls alle Paare P_i , Q_j , $1 \le i \le r$, $1 \le j \le s$ unabhängig bzgl. D sind.
- ii) (stark) unabhängig, falls alle Paare $P = \sum_{i \in I} P_i$, $Q = \sum_{j \in J} Q_j$ mit beliebigen $I \subseteq \{1, \ldots, r\}$, $J \subseteq \{1, \ldots, s\}$ unabhängig bzgl. D sind.

Aus ii) folgt natürlich i). Die Umkehrung gilt i.A. aber nicht:

2.6. BEISPIELE:

i) Sei in einer festen Basis des ℂ³ der reine Zustand D die Proj.–

$$\text{Matrix: } \mathbf{D} = \mathbf{P_d} = \frac{\mathbf{1}}{\mathbf{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \text{ auf den von } \mathbf{d} = \sqrt{\frac{\mathbf{1}}{\mathbf{3}}} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \text{ aufgespannten Teilraum.}$$

A und B sollen jeweils drei verschiedene Eigenwerte haben, mit assoziierten Projektionen P_i , Q_j $1 \le i,j \le 9$ auf eindim. Teilräume, die durch (normierte) Eigenvektoren p_i , q_j aufgespannt werden:

$$\mathbf{p_i} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad \mathbf{p_z} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \quad \mathbf{p_s} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \qquad \mathbf{q_i} = \sqrt{\mathbf{a}} \begin{bmatrix} 1 \\ \lambda \\ \lambda \end{bmatrix} \quad \mathbf{q_z} = \sqrt{\mathbf{a}} \begin{bmatrix} 1 \\ \lambda \\ 1 \end{bmatrix} \quad \mathbf{q_s} = \sqrt{\mathbf{a}} \begin{bmatrix} 1 \\ 1 \\ \lambda \end{bmatrix} \quad \lambda = e^{\mathbf{i}\mathbf{2}\pi/\mathbf{a}}$$

Unter Verwendung von (2.3) folgt:

$$\text{tr}(P_iQ_jP_iD) = \left| \langle P_i | q_j \rangle \right|^2 \text{tr}(P_iD) = \left| \langle P_i | q_j \rangle \right|^2 \left| \langle P_i | d \rangle \right|^2 = \frac{4}{9}$$
 ebenso ist
$$\text{tr}(Q_jP_iQ_jD) = \frac{4}{9}$$

$$\operatorname{tr}(P_iD) = |\langle p_i | d \rangle|^2 = \frac{1}{3}$$
, ebenso $\operatorname{tr}(Q_iD) = \frac{1}{3}$

je für alle $4 \le i,j \le 3$. In (2.7) eingesetzt zeigt dies, daß alle Paare P_i , Ω_j unabhängig, und damit A und B schwach unabhängig bzgl. D sind.

Betrachten wir nun die beiden Projektionsoperatoren $P_1 + P_2$ und Q_1 :

$$\text{tr}\,(Q_{_{\bm{1}}}(P_{_{\bm{1}}}+P_{_{\bm{2}}})\,Q_{_{\bm{1}}}D) \ = \ \text{tr}\,(Q_{_{\bm{1}}}P_{_{\bm{2}}}Q_{_{\bm{1}}}D) + \text{tr}\,(Q_{_{\bm{1}}}P_{_{\bm{2}}}Q_{_{\bm{1}}}D) \ = \ \frac{2}{9}$$

aber z.B. explizites Einsetzen der Matrizen zeigt sofort:

$$tr((P_1+P_2)Q_1(P_1+P_2)D) = \frac{1}{9}$$

Bereits der erste Teil von (2.7), die Unabhängigkeit der Reihenfolge der Messungen ist nicht mehr erfüllt. Mit der Notation von (2.6):

$$\mu_{\mathbf{p}}((\mathbf{P_4} + \mathbf{P_2}) \cap \mathbf{Q_4}) \neq \mu_{\mathbf{p}}(\mathbf{Q_4} \cap (\mathbf{P_4} + \mathbf{P_2}))$$

Schuld ist das Auftreten sogen. Interferenzeffekte der Wahrscheinlichkeitsamplituden. A. B sind also nicht stark unabhängig bzgl. D.

ii) Ist $D=\frac{1}{n}1$, liegt der (klassische) Fall kommutierender A und B vor, oder haben A und B jeweils nicht mehr als zwei verschiedene Eigenwerte, so genügt bereits die schwache Unabhängigkeit bzgl. D um auch auf die starke schließen zu können. Abgesehen von diesen Spezialfällen sind aber die Bedingungen dafür so einschränkend, daß nicht klar ist ob weitere Lösungen für starke Unabhängigkeit existieren. Wir geben darum eine solche an:

Seien im \mathbb{C}^4 die selbstadjungierten A und B mit je vier verschiedenen Eigenwerten, so gewählt, daß P_1,\ldots,P_4 auf die jeweils von den Standard-Basisvektoren aufgespannten Teilräume projizieren, Ω_1,\ldots,Ω_4 auf die von den Spalten von H aufgespannten Teilräume:

Es läßt sich leicht nachprüfen, daß A und B bzgl. der Dichtematrix D stark unabhängig sind. (Interferenzterme kürzen sich hier weg).

Folgendes war eine Hilfe beim Auffinden dieser Lösungen und zeigt auch die besondere Rolle von $D=\frac{1}{D}1$.

2.7. Proposition: A und B seien nichtentartete, selbstadjungierte n×n Matrizen, schwach unabhängig bzgl. einer (strikt) positiven Dichtetematrix D. Dann sind A und B auch unabhängig bzgl. $\frac{1}{n}$ 1.

Bew.: Nichtentartet heißt: A und B haben Projektionen P_i , Q_j auf eindimensionale Teilräume. Wieder mit (2.3) wird (2.7) zu:

$$\text{tr}(P_i^{}Q_i^{})\,\text{tr}(P_i^{}D) \;=\; \text{tr}(P_i^{}Q_i^{})\,\text{tr}(Q_i^{}D) \;=\; \text{tr}(P_i^{}D)\,\text{tr}(Q_i^{}D)$$

Weil D (strikt) positiv ist, d.h. $\langle e|De \rangle > \emptyset$ $\forall e \in \mathbb{C}^n$ gilt, folgt: $\operatorname{tr}(P_iD) \neq \emptyset$, $\operatorname{tr}(Q_jD) \neq \emptyset$ und damit auch: $\operatorname{tr}(P_iQ_j) \neq \emptyset$

und die Gleichung kürzt sich zu:

$$\begin{array}{ll} & \text{tr}(P_iD) = \text{tr}(Q_jD) = \text{tr}(P_iQ_j) \\ \\ \Rightarrow & \text{n.tr}(P_iD) = \sum\limits_{j=1}^n \text{tr}(P_iD) = \sum\limits_{j=1}^n \text{tr}(Q_jD) = \text{tr}(D) = 1 \\ \\ \Rightarrow & \text{tr}(P_iD) = \text{tr}(P_iQ_j) = \frac{1}{n} \quad \text{für alle 1} \leq i,j \leq n \end{array}$$

Die Vorraussetzungen sind notwendig. Sind z.B. A und B entartet, gibt es bereits in der klassischen Wahrscheinlichkeitstheorie und also für kommutierende Matrizen einfache Gegenbeispiele: $\text{Im } \mathbb{C}^5 \colon \text{Sei D=diag}(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{8},\frac{1}{8}), \ P_1 = \text{diag}(1,1,0,0,0), \ P_2 = 1-P_1, \\ Q_1 = \text{diag}(1,0,1,0,0), \ Q_2 = 1-Q_1, \ \text{so sind P}_1 \ \text{und Q}_j \ \text{für } 1 \le i,j \le 2 \ \text{unabhängig bzgl. D, aber nicht bzgl.}$

Andererseits gibt es in der klassischen Wahrscheinlichkeitstheorie eine zu Prop. 2.7 völlig analoge Situation:

2.8. PROPOSITION: Sei $\Omega = \{\omega_1, \ldots, \omega_n\}$ eine n-elementige Menge und $\nu(\omega_i) > \emptyset$, ($1 \le i \le n$) ein (strikt) positives Wahrscheinlichkeitsmaß. Seien f bzw. g Zufallsvariablen über Ω mit r bzw. s verschiedenen Werten, sodaß n=r.s ist. Sind f und g unabhängig bzgl. ν , so folgt, daß sie auch bzgl. $\mu(\omega_i) = \frac{1}{n}$ ($1 \le i \le n$) unabhängig sind.

Bew.: Seien die Werte von $\mathbf{f}: \mathbf{x_i}, \dots, \mathbf{x_r}$ und von $\mathbf{g}: \mathbf{y_i}, \dots, \mathbf{y_s}$. Da für $\mathbf{f}^{-1}(\mathbf{x_i}) \neq \{\}$ und $\mathbf{g}^{-1}(\mathbf{y_j}) \neq \{\}$ und ν strikt positiv ist,

$$\begin{split} &\text{folgt:} \quad \nu\Big[\mathbf{f}^{-1}(\mathbf{x}_i) \ \cap \ \mathbf{g}^{-1}(\mathbf{y}_j)\Big] = \nu\Big[\mathbf{f}^{-1}(\mathbf{x}_i)\Big], \nu\Big[\mathbf{g}^{-1}(\mathbf{y}_j)\Big] > \emptyset \\ &\text{also ist:} \qquad \mathbf{f}^{-1}(\mathbf{x}_i) \ \cap \ \mathbf{g}^{-1}(\mathbf{y}_j) \neq \{\} \qquad \qquad \text{für } 1 \leq i \leq r, \ 1 \leq j \leq s \,. \\ &\text{Das sind r.s=n disjunkte, nichtleere Mengen in } \Omega, \ d.h. \ sie \ enthalten \ \text{je genau ein Element:} \qquad \Big|\mathbf{f}^{-1}(\mathbf{x}_i) \ \cap \ \mathbf{g}^{-1}(\mathbf{y}_j)\Big| = 1 \\ &|\mathbf{f}^{-1}(\mathbf{x}_i)| = \sum_{j=1}^s |\mathbf{f}^{-1}(\mathbf{x}_i) \ \cap \ \mathbf{g}^{-1}(\mathbf{y}_j)\Big| = s, \qquad \text{ebenso:} \qquad \Big|\mathbf{g}^{-1}(\mathbf{y}_j)\Big| = r \end{split}$$

Damit ist Glong. (1.1) für alle ±≤i≤r und ±≤j≤∍ erfüllt

Wesentlich war in beiden Fällen, daß eine maximale Anzahl verschiedener Werte, einerseits von A und B (nichtentartet, d.h. je n verschiedene Eigenwerte), andererseits von f und g (r.s=n), gefordert wurde.

Prop. 2.7 legt nahe, Lösungen, die den dort angeführten Bedingungen gehorchen, durch zwei Schritte zu bestimmen:

- i) Suche alle bzgl. $\frac{1}{n}$ unabhängigen, nichtentarteten A und B
- ii) Finde alle D, welche $\operatorname{tr}(P_iD) = \operatorname{tr}(Q_jD) = \frac{1}{n} \ (1 \le i, j \le n)$ erfüllen. Dies sind alle D bzgl. denen A und B schwach unabhängig sind. Sie bilden eine konvexe Menge und eine ebenfalls konvexe Teilmenge davon bilden jene bzgl. denen sie stark unabhängig sind.
- 2.9. Lemma: Selbstadjungierte Matrizen A und B sind unabhängig bzgl. $\frac{1}{n}$ genau dann, wenn es $\alpha_i \in \mathbb{R}$, $1 \le i \le r$ und $\beta_j \in \mathbb{R}$, $1 \le j \le s$ gibt, sodaß:

$$tr(P_iQ_j) = \alpha_i\beta_j$$
 für alle $i \le i \le r$, $i \le j \le s$

 $\mathsf{Bew.:} \Rightarrow) \mathsf{\ Setze\ } \alpha_{_{\!i}} = \mathsf{tr}(\mathsf{P}_{_{\!i}}) \, / \mathsf{n} \, , \, \, \beta_{_{\!j}} = \mathsf{tr}(\mathsf{Q}_{_{\!j}}) \, , \, \, (\alpha_{_{\!i}} \, , \, \, \beta_{_{\!j}} \, \, \mathsf{sind\ nicht\ eindeutig})$

←) es folgt dann:

$$\operatorname{tr}(P_{i}Q_{j})\operatorname{tr}(P_{k}Q_{l}) = \operatorname{tr}(P_{i}Q_{l})\operatorname{tr}(P_{k}Q_{i})$$

für alle ≤≤i,k≤r, ≤≤j,l≤s

Summation über $\sum_{k=1}^{r}$ und über $\sum_{k=1}^{s}$ ergibt Glchg.(1.4)

Für die Unabhängigkeit bzgl. $D=\frac{1}{n}$ 1 genügt es also zu fordern, daß die gemeinsame Wahrscheinlichkeit $\mu_{_{\mathbf{D}}}(P_{_{\mathbf{I}}} \cap \Omega_{_{\mathbf{J}}}) = \mu_{_{\mathbf{D}}}(\Omega_{_{\mathbf{J}}} \cap P_{_{\mathbf{I}}}) = \operatorname{tr}(P_{_{\mathbf{I}}} \Omega_{_{\mathbf{J}}})$ sich irgendwie als Produktmaß schreiben läßt. Daran knüpfen wir im nächsten Abschnitt an.

2.3. IN UNENDLICHDIMENSIONALEN HILBERTRÄUMEN

Im Anschluß an Def.2.5 läßt sich (starke) Unabhängigkeit zweier selbstadjungierter Operatoren A und B über einem separablen Hilbertraum № bzgl. einem Dichteoperatoren D durch folgende Forderung definieren. Die Spektralprojektionen:

$$\chi_{_{\rm I\!P}}({\rm A})$$
 und $\chi_{_{\rm I\!P}}({\rm B})$

sollen für beliebige Borelmengen $\mathbf{E},\mathbf{F}\subseteq\mathbb{R}$ unabhängig bzgl. D sein. Schwache Unabhängigkeit bzgl. D läßt sich nur für Operatoren mit rein diskretem Spektrum definieren.

Obige Forderung ist nicht leicht zu handhaben. Wir verfolgen die allgemeine Theorie hier nicht weiter, sondern überlegen uns wie der Speziallfall D∿1 zu retten ist.

Der Einheitsoperator 1 ist kein Dichteoperator. Mit $\mu_{\mathbf{1}}(P):=\operatorname{tr}(P)$ ist nur ein Maß auf den orthogonalen Projektionen auf endlichdim. Teilräume gegeben, daß nur noch (2.1.ii) und iii) erfüllt.

$$\mu_{\mathbf{i}}(P \cap Q) := tr(QPQ)$$
 und $\mu_{\mathbf{i}}(Q \cap P) := tr(PQP)$

-können aber auch für orthog. Projektionen P und Q auf unendlichdimensionale Teilräume endlich sein. Ist $\operatorname{tr}(P)<\infty$, oder $\operatorname{tr}(Q)<\infty$, können wir, wie auch im \mathbb{C}^n , mit Glchg.(2.2.v) argumentieren:

$$tr(QPQ) = tr(PQ) = tr(PQP)$$

Aber Achtung! Im allgemeinen folgt aus $\mathbf{QPQ} \in \mathcal{P}_{\mathbf{i}}$ (Spurklasse) nicht notwendig $\mathbf{PQ} \in \mathcal{P}_{\mathbf{i}}$. Wir können also nicht generell auf den Ausdruck $\mathrm{tr}(\mathbf{PQ})$ zurückgreifen. Wir geben ein Beispiel :

Sei \mathscr{R} als orthogonale Summe $\mathscr{R} = \ell_2 \oplus \ell_2$ und die Operatoren darauf als 2×2 Matrizen geschrieben, mit Einträgen, welche Operatoren von $\ell_2 \to \ell_2$ sind. Sei: $0 = \begin{bmatrix} 1 & 0 \end{bmatrix}$ $0 = \begin{bmatrix} c^2 & CD \end{bmatrix}$ (2.0)

$$\ell_2 \rightarrow \ell_2 \text{ sind. Sei:} \qquad Q = \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \qquad P = \begin{bmatrix} \mathbf{C}^2 & \mathbf{CD} \\ \mathbf{CD} & \mathbf{D}^2 \end{bmatrix} \qquad (2.9)$$

mit C=diag $(1,\frac{1}{2},\frac{1}{3},\ldots,\frac{1}{k},\ldots)$ und der Diagonalmatrix D, sodaß $C^2+D^2=1$ P und Q sind zwei Projektionsoperatoren über $\mathscr R$.

$$QPQ = \begin{bmatrix} C^2 & O \\ O & O \end{bmatrix}$$

QPQ = |QPQ| ist positiv semidefinit und darum (Reed/Simon [37],

Th.VI.18) seine Spur $\text{tr}(\mathbf{QPQ}) = \sum_{k=1}^{\infty} \frac{1}{k} \mathbf{z} = \frac{\pi}{6}$ basisunabhängig. \mathbf{QPQ} ist also Element von $\mathcal{P}_{\mathbf{z}}$, der Spurklasse. Aber:

Es gilt aber immer noch:

2.10. LEMMA: Für beliebige orthogonale Projektionen P und Q über einem separablen % gilt: tr(PQP) = tr(QPQ)

Bew.: Sei % als orthogonale Summe geschrieben (siehe Lenard [30]): $\mathscr{R} = \mathscr{R}_{00} \oplus \mathscr{R}_{10} \oplus \mathscr{R}_{10} \oplus \mathscr{R}'$

wobei \mathscr{R}_{nm} für $n_n m = 0.4$ aufgespannt wird von den gemeinsamen Eigenvektoren f von P und Q, welche Pf = nf und Qf = mf erfüllen. \mathscr{R}' ist das orthogonale Komplement der ersten vier Unterräume. P und Q kommutieren auf $\mathscr{R}'':=\mathscr{R}_{oo} \oplus \mathscr{R}_{o1} \oplus \mathscr{R}_{10} \oplus \mathscr{R}_{11}$. Da $tr(A)=tr(A|_{\mathscr{R}'})+tr(A|_{\mathscr{R}'})$ und das Lemma für kommutierende Operatoren erfüllt ist, muß es nur noch für $P|_{\mathscr{R}'}$ und $Q|_{\mathscr{R}'}$ gezeigt werden. Die beiden heißen in "generic position". Halmos [26] zeigte, daß sich beliebige P und Q in generic position immer auf die Gestalt (2.9) unitär transformieren lassen, mit positiven C und D deren Kern Null ist und die $C^2+D^2=1$ erfüllen. Mit dem unitären $U=\begin{bmatrix} C & D \\ D & -C \end{bmatrix}$ gilt dann $P=U^{-1}QU$ und $Q=U^{-1}PU$ PQP ist positiv semidefinit und damit die Spur basisunabhängig:

$$tr(PQP) = tr(U^{-1}PQPU) = tr(U^{-1}PUU^{-1}QUU^{-1}PU) = tr(QPQ)$$

Also ist $\mu_{\mathbf{1}}(\mathbf{P} \cap \mathbf{Q}) = \mu_{\mathbf{1}}(\mathbf{Q} \cap \mathbf{P})$. Diese Zahl läßt sich als Maß für die Gemeinsamkeit von P und Q interpretieren. (Kommutieren z.B. P, Q, ist $\mathrm{tr}(\mathbf{PQP})$ die Dimension des Durchschnitts der zugehörigen Teilräume).

Wir können jetzt, wie auch Lemma 2.9 nahelegt, Unabhängigkeit von selbstadj. Operatoren bzgl. 1 definieren, falls sich dieses Maß auf ihren Spektralprojektionen, irgendwie als Produktmaß schreiben läßt. Accardi [O1] fand einen analogen Ansatz, benützte dabei aber leider den Ausdruck tr(PQ).

2.11. DEFINITION: A und B seien zwei selbstadjungierte Operatoren über einem separablen Hilbertraum $\mathscr R$ mit Spektrum $\sigma(A)$ und $\sigma(B)$. Sie heißen unabhängig bzgl. 1, falls es Borelmaße μ_A auf $\sigma(A)$ und μ_B auf $\sigma(B)$ gibt, sodaß für beliebige kompakte Teilmengen $E\subseteq \sigma(A)$ und $F\subseteq \sigma(B)$ gilt:

$$tr(\chi_{\mathbf{E}}(\mathbf{A}), \chi_{\mathbf{F}}(\mathbf{B}), \chi_{\mathbf{E}}(\mathbf{A})) = \mu_{\mathbf{A}}(\mathbf{E}), \mu_{\mathbf{B}}(\mathbf{F})$$
 (2.10)

Falls ∞ endlichdimensional ist, stimmt diese Definition überein mit der Unabhängigkeit bzgl. ½1 (siehe Lemma 2.9, Prop. 2.4).

Erinnert sei daß für Borelmaße μ auf lokalkompakten Räumen für kompakte \mathbf{E} gilt: $\mu(\mathbf{E}) < \infty$ (Bauer [05], Def.43.3). Insbesondere muß also $\mathrm{tr}(\chi_{\mathbf{E}}(\mathbf{A}),\chi_{\mathbf{F}}(\mathbf{B}),\chi_{\mathbf{E}}(\mathbf{A})) < \infty$ sein für kompakte \mathbf{E} und \mathbf{F} .

2.12. BEISPIEL: Sei A ein selbstadjungierter Operator über einem Hilbertraum $\mathscr{R}_{\mathbf{1}}$, für den gilt: $\mathrm{tr}(\chi_{_{\mathbf{E}}}(\mathbf{A})) < \infty$ für bel. kompakte Teilmengen \mathbf{E} von $\mathscr{O}(\mathbf{A})$. B über $\mathscr{R}_{\mathbf{2}}$ erfülle dieselbe Eigenschaft.

A⊗1 und 1⊗B sind unabhängig bzgl. 1 über % ⊗ %2:

Da $\chi_{\mathbf{E}}(\mathbf{A}\otimes\mathbf{1})=\chi_{\mathbf{E}}(\mathbf{A})\otimes\mathbf{1}$ und ebenso $\chi_{\mathbf{F}}(\mathbf{1}\otimes\mathbf{B})=\mathbf{1}\otimes\chi_{\mathbf{F}}(\mathbf{B})$ folgt: $\operatorname{tr}(\chi_{\mathbf{E}}(\mathbf{A}\otimes\mathbf{1}),\chi_{\mathbf{F}}(\mathbf{1}\otimes\mathbf{B}),\chi_{\mathbf{E}}(\mathbf{A}\otimes\mathbf{1}))=\operatorname{tr}(\chi_{\mathbf{E}}(\mathbf{A})\otimes\chi_{\mathbf{F}}(\mathbf{B}))=\operatorname{tr}(\chi_{\mathbf{E}}(\mathbf{A})),\operatorname{tr}(\chi_{\mathbf{F}}(\mathbf{B}))$ (2.10) ist also erfüllt mit $\mu_{\mathbf{A}}(\mathbf{E})=\operatorname{tr}(\chi_{\mathbf{E}}(\mathbf{A}))$ und $\mu_{\mathbf{F}}(\mathbf{B})=\operatorname{tr}(\chi_{\mathbf{F}}(\mathbf{B}))$.

Die Tensorproduktbildung wird in der Quantenmechanik benützt um Eigenschaften völlig getrennter, unabhängiger Systeme zu beschreiben. Die technischen Vorraussetzungen in obigem Beispiel sind aber im Rahmen unserer Theorie leider nötig. Wollten wir beliebige A01 und 10B für unabhängig bzgl. 1 erklären, müßten wir die Definition 2.11 so abändern, daß (2.10) auch als erfüllt gilt, falls beiderseits ∞ steht. Dies würde aber zu große Beliebigkeit der Lösungen zur Folge haben.

Mit A und B sind auch f(A) und g(B) unabhängig bzgl. 1, unter der techn. Vorraussetzung, daß für die reellwertige Funktion f gilt: $f^{-1}(\mathbf{E}) \text{ ist kompakt in } \sigma(\mathbf{A}), \text{ falls } \mathbf{E} \text{ kompakt in } \sigma(f(\mathbf{A})) \text{ ist. Analog für g. Geeignetes Maß auf } \sigma(f(\mathbf{A})) \text{ ist dann } \mu_{f(\mathbf{A})}(\mathbf{E}) := \mu_{\mathbf{A}}(f^{-1}(\mathbf{E})).$

Die folgende Lösung wurde auch von Accardi [01] (für eine leider inkorrekte Glchg.) angegeben. In einem anderen Zusammenhang, wird auch bei Amrein/Berthier [03], Glchg.(11), die wesentliche Formel (bis auf einen Faktor */2n) notiert.

Sei $\mathscr{R}=\mathscr{L}^2(\mathbb{R})$. Für $\mathbf{f}\in\mathscr{R}$ sei Ff die fouriertransformierte Funktion: $(\mathbf{F}\mathbf{f})_{(p)}=\sqrt{\frac{i}{2\pi}}\int\limits_{-\infty}^{\infty}e^{-i\times p}\mathbf{f}_{(x)}\mathrm{d}x$

Die selbstadj. Operatoren X und P sind auf dichten Teilräumen von $\mathscr{Z}^2(\mathbb{R})$ definiert durch:

$$(Xf)(x) = xf(x)$$
 DZW . $(FPf)(p) = p(Ff)(p)$

Eine kurze Rechnung gibt: $P = -i\frac{d}{dx}$.

2.13. Proposition: X und P sind unabhängig bzgl. 1

Bew.: Seien ⊑ und ⋤ kompakte (Borel-)Teilmengen von ℝ.

$$\begin{array}{lll} \operatorname{tr} \left(\chi_{_{\mathbf{E}}} \left(\mathbf{X} \right) , \chi_{_{\mathbf{F}}} \left(\mathbf{P} \right) , \chi_{_{\mathbf{E}}} \left(\mathbf{X} \right) \right) &= \operatorname{tr} \left(\mathbf{A}^{*} \mathbf{A} \right) & \operatorname{mit} & \mathbf{A} := \mathbf{F} , \chi_{_{\mathbf{F}}} \left(\mathbf{P} \right) , \chi_{_{\mathbf{E}}} \left(\mathbf{X} \right) \\ & \left(\mathbf{A} \mathbf{f} \right) \langle \mathbf{p} \rangle &= \chi_{_{\mathbf{F}}} \langle \mathbf{p} \rangle \sqrt{\frac{1}{2\pi}} \int\limits_{-\infty}^{\infty} \mathrm{e}^{-\mathrm{i} \mathbf{x} \mathbf{p}} \chi_{_{\mathbf{E}}} \langle \mathbf{x} \rangle \mathbf{f} \langle \mathbf{x} \rangle \mathrm{d} \mathbf{x} \end{array}$$

Die Hilbert-Schmidt Norm $(\operatorname{tr}(\operatorname{A}^*\operatorname{A}))^{1/2}$ eines Integraloperators A existiert, falls dessen Integralkern im $\mathscr{L}^2(\mathbb{R}^2)$ ist und ist gleich dessen $\mathscr{L}^2(\mathbb{R}^2)$ -Norm (siehe Reed/Simon, Theorem VI.23). Also folgt:

mit dem Lesbesgue-Borelmaß λ auf $\mathbb R$.

Die Operatoren X und $P=-i\frac{d}{dx}$ repräsentieren in der Quantenmechanik die Orts- bzw. die Impulsobservable. Dies sind in der klassischen Mechanik völlig unabhängige Größen (bzgl. eines homogenen Phasenraumes). Es gibt mehrer Gründe für diesen Ansatz (z.B. Darstellungstheorie der Weylalgebra, Unschärferelation). Seinen wahrscheinlichkeitstheoretischen Hintergrund herauszuarbeiten war ursprünglicher Anlaß dieser Arbeit.

Wir definieren für beliebige $\alpha \in [0,\pi)$ selbstadjungierte Operatoren auf einem dichten Teilraum von $\mathcal{Z}^{\mathbf{Z}}(\mathbb{R})$ durch:

2.14. PROPOSITION: \mathbf{A}_{α} und \mathbf{A}_{α} , sind unabhängig bzgl.1, für $\alpha \not= \alpha'$, $\alpha, \alpha' \in [0, \pi)$. Das heißt: Die \mathbf{A}_{α} bilden eine unendliche Menge paarweise bzgl. 1 unabhängiger, selbstadj. Operatoren.

Bew.: Für r,s∈R seien unitäre Operatoren U_,V_ definiert durch:

$$(U_{r}f)(x) := e^{irx^{2}/2}f(x)$$
 $(FV_{s}f)(p) := e^{isp^{2}/2}(Ff)(p)$

Eine kurze Rechnung zeigt:

$$U_r^{-1}XU_r = X$$
 $V_s^{-1}PV_s = P$
 $U_r^{-1}PU_r = rX + P$ $V_s^{-1}XV_s = X - SP$

Sei c:=cos(α)≠Ø, sonst vertauschen wir α und α' und sei s:=-tan(α)

$$\Rightarrow \qquad V_{s}^{-1}A_{\alpha V_{s}} = cX \qquad V_{s}^{-1}A_{\alpha V_{s}} = (cos(\alpha'))X + dP$$

mit $d = \cos(\alpha')\tan(\alpha) - \sin(\alpha') \neq \emptyset$ nach Vorr. Sei nun $r:=-\cos(\alpha')/d$,

$$\Rightarrow \qquad U_r^{-1}V_s^{-1}A_{\alpha}V_sU_r = CX \qquad \qquad U_r^{-1}V_s^{-1}A_{\alpha}, V_sU_r = dP$$

Das heißt: Aα und Aα, sind für α≠α' unitär äquivalent zu den paarweise bzgl. 1 unabhängigen Operatoren cX und dP (c,d≠0). Daraus folgt natürlich, daß sie selbst unabhängig bzgl. 1 sind.

Dieselbe Methode liefert noch weitere solcher Lösungen. (Ein Resultat von Wiesbrock [49], p.1179 ergibt z.B. zusammen mit dem obigen, daß {X²+aX+bP, a∈R}, für bel. festes b∈R/{0} eine Schar paarw. bzgl. 1 unabhängiger Operatoren bilden).

Unsere Lösung ist aber besonders interessant, da sie eine Übertragung ins Endlichdimensionale gestattet. Dazu müssen wir sie anders beschreiben.

Wir ordnen \mathbf{A}_{α} eine einparametrige, (stark stetige) Gruppe unitärer Operatoren zu: $\mathbf{U}_{\alpha}(t):=\exp(i\mathbf{A}_{\alpha}t)$ telR

Die infinitesimalen Generatoren A_{α} sind durch die $U_{\alpha}(t)$, telk eindeutig bestimmt: $iA_{\alpha} = \lim_{h \to 0} (\frac{1}{h}(U_{\alpha}(h)-1))$

Eine kurze Rechnung zeigt, daß mit $r:=t.sin(\alpha)$ und $s:=t.cos(\alpha)$ gilt:

$$U_{\alpha}(t) = W(r,s) = e^{-irs/2}e^{irP}e^{isX}$$
 (2.11)

 $\alpha \in [0, \pi)$, tel \Leftrightarrow r, sel.

Die Operatoren W(r,s) heißen Weyl-operatoren (Thirring [43], p.76). Diese lassen sich also durch 'Polarkoordinaten': α,t in unitäre, einparametrige (⇒kommutative) Gruppen zerlegen, die jeweils einen von unendlich vielen paarweise bzgl. 1 unabhängigen Operatoren festlegen.

Hermann Weyl [48] führte diskrete Gegenstücke der nach ihm benannten Operatoren ein und zwar als eindeutige irreduzible Strahldarstellungen der Gruppe ($\mathbb{Z}_n \times \mathbb{Z}_n$,+) durch komplexe n×n Matrizen. Diese Matrizen bilden die Grundbausteine der Konstruktion in Kapitel 4, die diverse vollständige Lösungen von paarweise bzgl. $\frac{1}{n}$ 1 unabhängigen Matrizen liefert.

3. ÄQUIVALENZEN, SCHRANKEN

Dieses Kapitel stellt vor allem die (technischen) Grundlagen zur Verfügung für das Problem k-tupel paarweise bzgl. ½1 unabhängiger, selbstadjungierter n×n Matrizen zu bestimmen. Die Äquivalenzdefinitionen ergeben sich völlig natürlich. Eine geometrische Interpretation liefert eine neue Formulierung. Daraus folgen dann sofort Ungleichungen. Das Tensorprodukt ist ein wichtiges Konstruktionsprinzip. Reduziert auf die in Kap.1 angeführten Speziallfälle erhalten wir Jeweils bekannte Ansätze und Formeln.

3.1. ÄQUIVALENZEN

- 3.1 **DEFINITION**: Zu k paarweise bzgl. $\frac{1}{n}$ 1 unabhängigen, selbstadj. n×n Matrizen A_1, \ldots, A_k sind A_1', \ldots, A_k' äquivalent, falls sie durch beliebige Hintereinanderausführung folgender Operationen daraus hervorgehen:
- i) Alle A_i $1 \le i \le k$ werden gleichzeitig durch eine unitäre $n \times n$ Matrix U transformiert: $A_i' = U^{-1}A_iU$ für alle $1 \le i \le k$
- ii) Die verschiedenen Eigenwerte der Α werden beliebig verändert, aber so, daß sie auch verschieden bleiben.
- iii) Die Reihenfolge der $\mathbf{A_1}, \dots, \mathbf{A_k}$ wird beliebig permutiert. Das sind k! Möglichkeiten.

Eigenwerte spielen keine Rolle, sondern einzig die zugeordneten Eigenraumprojektionen. Das ist jeweils eine Zerlegung der Einheitsmatrix in orthogonale Projektionsmatrizen. Wir könnten die Definition gleich nur darauf beziehen. Die geschlossene Notation durch selbstadjungierten Matrizen bzw. folgende Erweiterung davon ist aber oft nützlich.

Eine komplexe n×n Matrix A heißt normal, falls gilt: AA^{*}= A^{*}A. Äquivalent dazu ist, daß es eine unitäre Matrix V gibt, sodaß V⁻¹AV diagonal ist. (Hoffman/Kunze [29], § 8.5). Das ist wieder gleichbedeutend damit, daß es eine Zerlegung der Einheitsmatrix in orthogonale Projektionsmatrizen P_i , $1 \le i \le r$ gibt: $P_i P_j = \delta_{ij} P_i$ und $\sum_{i=1}^r P_i = 1$, sodaß $A = \sum_{i=1}^r a_i P_i$, wobei $a_i \in \mathbb{C}$ die verschiedenen Eigenwerte von A sind.

Wir könnten folglich unsere Definition der Unabhängigkeit bzgl.

1 auch auf normale, statt nur selbstadjungierte Matrizen beziehen. In ii) lassen wir dann bel. Veränderung der komplexen Eigenwerte, aber so daß sie verschieden bleiben, zu. Wir erhalten so größere, aber nicht mehr Äquivalenzklassen. In jeder solchen liegen auch Lösungen mit selbstadj. Matrizen. Andere Vertreter sind aber oft praktischer.

Letztendlich kann man die Definition auch jeweils auf alle Linear-kombinationen: $\sum_{i=1}^{n} a_i P_i$, $a_i \in \mathbb{C}$ gleichzeitig beziehen. Das ist ein r-dimensionaler Teilraum von kommutierenden Matrizen, die sich alle als Funktion einer Matrix schreiben lassen. (siehe nächster Abschn.)

Kommutieren die A_i paarweise, können sie mit i) alle gleichzeitig diagonalisiert werden, wobei durch (unitäre) Permutationsmatrizen eine beliebige Anordnung der Diagonalpunkte erreicht werden kann.

Ein Speziallfall der so erhaltenen, bzgl. der Gleichverteilung unabhängigen klassischen Zufallsvariablen, wird durch Lateinische
Quadrate beschrieben (siehe Kap.1 Abschnitt 1). Durch die Festlegung der Werte (Einträge) mit 0,1,...,r-1 bleibt von ii) nur
noch die beliebige Permutation von Zeilen, Spalten bzw. Einträgen.
Das entspricht dem Konzept der Isotopy. iii) entspricht der Bildung
sogenannter konjugierter oder parastropher Lateinischer Quadrate.
Man spricht zusammen von der Bildung sogenannter Hauptklassen.
(Dénes/Keedwell [20], §1.3,§2.2,§4.1,§4.2).

Beschränken wir uns jetzt einmal auf nur zwei bzgl. $\frac{1}{n}$ 1 unabhängige selbstadjungierte n×n Matrizen A und B mit Eigenraumprojektionen P_i , $1 \le i \le r$ bzw. Q_j , $1 \le j \le s$. A habe geordnete Diagonalgestalt. Eine unitäre Matrix \mathbf{U} , die B in $\hat{\mathbf{B}} = \mathbf{U}^{-1}\mathbf{B}\mathbf{U}$,mit ebenfalls geordneter Diagonalgestalt transformiert, ist eine A und B zugeordnete VBH-Matrix, mit $k_i \times l_j$ Submatrizen \mathbf{U}_{ij} ($k_i = \operatorname{tr}(P_i)$ und $l_j = \operatorname{tr}(Q_j)$).

Sei V eine unitäre Matrix, die mit A kommutiert. W eine unitäre Matrix, die mit B kommutiert. Wir hätten auch von $VAV^{-1} = A$ und VBV^{-1} ausgehen können und U' = VUW zuordnen:

$$U'^{-1}(VBV^{-1})U' = \hat{B}$$

vuw ist die allgemeinste Form der A und B zugeordneten VBH-Matrizen. **v** kommutiert mit A, d.h. mit allen P_i . **v** hat folglich entlang der Diagonale unitären $k_i \times k_i$ Submatrizen v_i stehen (die mit $P_i v_i$ aus **v** "herausgeschnitten" werden) und sonst überall Nullen. Analog hat **w** unitäre $l_j \times l_j$ Submatrizen v_j entlang der Diagonale sonst Nullen. Die unitären v_i bzw. v_j sind beliebig. Sind v_i die v_i Submatrizen von v_j , so folgt:

$$U'_{i,j} = V_i U_{i,j} W_j$$
 $1 \le i \le r$, $1 \le j \le s$

Diese Transformationen ersetzen Punkt i) der vorigen Definition. Von ii) wurden die Eigenwerte erst gar nicht berücksichtigt. Es wurden aber die Eigenraumrojektionen P_i bzw. Q_j mit Indizes versehen, z.B. in aufsteigender Reihenfolge der Eigenwerte. Diese werden dann durch ii) beliebig permutiert. Das wird zur beliebigen Permutation der Indizes von $\mathbf{U}_{i,j}$, d.h. der Blockspalten bzw. Blockzeilen. iii) ergibt die inverse Matrix.

- 3.2. **DEFINITION**: Zu einer VBH-Matrix \mathbf{V} mit Partition: $k_{\mathbf{i}}+\ldots+k_{\mathbf{r}}=n$ und $l_{\mathbf{i}}+\ldots+l_{\mathbf{s}}=n$, d.h. $k_{\mathbf{i}}\times l_{\mathbf{j}}$ Submatrizen $\mathbf{V}_{\mathbf{i}\mathbf{j}}$ sind \mathbf{V}' äquivalent, die durch beliebige Hintereinanderausführung folgender Operationen daraus hervorgehen:
- i) Beliebige Zeilen/Spalten von ♥ in Blocknotation werden mit bel. unitären Matrizen von links/rechts multipliziert, d.h.:

$$\mathbf{U}_{i\,j}^{\prime} = \mathbf{V}_{i}\mathbf{U}_{i\,j}$$
 für alle $\mathbf{1} \leq \mathbf{j} \leq \mathbf{s}$

mit beliebigen unitären $k_i \times k_i$ Matrizen \mathbf{V}_i für bel. $\mathbf{1} \leq i \leq r$ und/oder $\mathbf{U}_{i,j}' = \mathbf{U}_{i,j} \mathbf{W}_j$ für alle $\mathbf{1} \leq i \leq r$

mit beliebigen unitären l_j×l_j Matrizen ₩_j für beliebige ±≤j≤r.

- ii) Die Spalten und/oder Zeilen der Matrix in Blocknotation werden beliebig permutiert. Das sind r!s! Möglichkeiten.
- iii) Invertieren: $U' = U^{-1}$

Es ist leicht direkt nachzuprüfen, daß i)→iii) wieder VBH-Matrizen ergeben.ii) und iii) verändern natürlich i. A. die Partitionen.

Für VH-Matrizen wird i) einfach zur beliebigen Multiplikation von Zeilen/Spalten mit komplexen Zahlen mit Betrag 1. Dies kann dazu benützt werden die Einträge der ersten Zeile und der ersten Spalte alle zu $+\sqrt{\frac{1}{n}}$ zu machen.

Für Hadamard-Matrizen nennt Wallis i) und ii) zusammen H-Äquivalenz. (Wallis [46], §10). iii) wäre hier die Transposition der Matrix. Werden die Einträge der ersten Zeile und Spalte alle zu +1 gemacht, nennt man die Hadamard-Matrix normalisiert.

Seien die Blöcke der VBH-Matrix alle quadratisch. Wir können dann mithilfe der Polarzerlegung (Hoffman/Kunze [29], Chap.9 Th.14) eine allgemeine Definition einer normalisierten Gestalt geben:

Für jede komplexe (quadr.) Matrix M gibt es eine unitäre Matrix \mathbf{U} (i.A. nicht eindeutig) und eine eindeutige positiv semidefinite Matrix N, sodaß $\mathbf{UM} = \mathbf{N}$. Analog gibt es \mathbf{U}' und \mathbf{N}' sodaß $\mathbf{MU}' = \mathbf{N}'$.

Wir können also i) benützen die (quadr.) Submatrizen der ersten Block-zeile bzw. -spalte alle zu positiv semidefiniten Matrizen zu machen. Da es weiters für jede Matrix M unitäre Matrizen U und V gibt, sodaß UMV = D diagonal und pos. semidef. ist, kann dabei U1 sogar zu einer pos. semidef. Diagonalmatrix gemacht werden. Für VBH-Matrizen mit nichtquadr. Blöcken sind entsprechende (techn.) Verallgemeinerungen der Normalform möglich.

3.3. Lemma: Jeder Äquivalenzklasse von bzgl. $\frac{1}{n}$ 1 unabhängigen, selbstadjungierten Matrizen A und B ist genau eine Äquivalenzklasse von VBH-Matrizen (mit Partition $k_i = tr(P_i)$ und $l_j = tr(Q_j)$) zugeordnet.

Zum Bew.: Die Zuordnung von \mathbf{U} zu \mathbf{A} und \mathbf{B} erfolgt wie in Kap.1. Zur Umkehrung wird von diagonalen Proj. \mathbf{P}_i und \mathbf{Q}_j , entsprechend den Partitionen ausgegangen und $\mathbf{Q}_j = \mathbf{U} \mathbf{\hat{Q}}_j \mathbf{U}^{-1}$ gebildet. Die Eigenwerte können beliebig (aber verschieden zu jedem \mathbf{P}_i bzw. \mathbf{Q}_j) gewählt werden. Die Verträglichkeit der Äquivalenzklassenbildung ist entsprechend den Bemerkungen vor Def.3.2. leicht nachzuprüfen.

Kurz noch allg. zu k paarweise bzgl. $\frac{1}{n}$ 1 unabhängigen, selbstadj. Matrizen: $\mathbf{A_i},\ldots,\mathbf{A_k}$. Ihnen ordneten wir k-1 VBH-Matrizen $\mathbf{U_i},\ldots,\mathbf{U_{k-1}}$ mit Produkteigenschaft zu. Die Partition von $\mathbf{U_i}$ entspricht dabei den Eigenraumdimensionen von $\mathbf{A_i}$ und $\mathbf{A_{i+1}}$. Es werden also für alle $\mathbf{U_i}$ jeweils gleich viele Zeilen zusammengefaßt, Spalten jeweils anders.

- 3.2' **DEFINITION**: Äquivalenztransformationen der $\mathbf{U_1}, \dots, \mathbf{U_{k-1}}$ verall-gemeinern Def.3.2 dergestalt:
- i) Beliebige unitär Matrizen V_i (mit Ordnung entsprechend der Dimension des i-ten Eigenraums von A_i) wirken auf die i-te Blockzeile <u>aller</u> V_i , $1 \le l \le k-1$ gleichzeitig von links.

Beliebige unitäre Matrizen $W_j^{(l)}$ (mit Ordnung entsprechend der Dimension des j-ten Eigenraums von A_{l+1}) wirken jeweils nur auf die j-te Blockspalte von U_l von rechts für bel. $1 \le l \le k-1$.

- ii) Die Blockzeilen der Matrizen werden alle gleichzeitig beliebig permutiert (r_i ! Möglichkeiten). Blockspalten können für jede Matrix einzeln bel. permutiert werden. Zusammen $\prod_{i=1}^k (r_i)!$ Möglichkeiten.
- iii) Die Reihenfolge der $\mathbf{U_i}, \dots, \mathbf{U_{k-i}}$ wird bel. permutiert und/oder: für ein bel. festes $1 \le i \le k-1$:

$$(\textbf{U}_{\underline{\textbf{1}}}\,,\,\dots\,,\,\textbf{U}_{\underline{\textbf{k}}-\underline{\textbf{1}}}) \ \rightarrow \ (\textbf{U}_{\underline{\textbf{i}}}^{-\underline{\textbf{1}}}\,,\ \textbf{U}_{\underline{\textbf{i}}}^{-\underline{\textbf{1}}}\textbf{U}_{\underline{\textbf{j}}} \ (\underline{\textbf{1}} \leq \underline{\textbf{j}} \leq \underline{\textbf{k}}-\underline{\textbf{1}}\,,\,\underline{\textbf{j}} \not\cong \underline{\textbf{i}})$$

(Vertauscht $\mathbf{A_i}$ und $\mathbf{A_{i+1}}$). Das sind insgesammt k! Möglichkeiten.

Punkt i) kann jetzt dazu benützt werden die Submatrizen der ersten Blockzeilen aller Matrizen, aber nur noch die erste Blockspalte einer einzigen Matrix (i.A. $\mathbf{U_i}$) positiv semidefinit zu machen.

Es ist leicht sich von der Richtigkeit folgender Verallgemeinerung von Lemma 3.3. zu überzeugen:

3.3' LEMMA: Jeder Äquivalenzklasse von k paarweise bzgl. $\frac{1}{n}$ 1 unabhängigen selbstadj. Matrizen ist eindeutig genau eine Äquivalenzklasse von k-1 VBH-Matrizen mit Produkteigenschaft zugeordnet.

Die Problemstellung ist jetzt also: Bestimme für jedes n und k und k beliebige Zerlegungen von n, die Anzahl dieser Äquivalenzklassen und je einen Repräsentanten aus jeder.

Ein Teilproblem wird durch die Zusatzforderung definiert, daß in der Darstellung durch selbstadjungierte Matrizen diese kommutieren sollen.

Ein Beispiel:

Sei mit $A_{n,k}$ die Anzahl der Äquivalenzklassen bezeichnet für nichtentartete A_i , bzw. VH-Matrizen V_i . Die ersten Werte von A_{nk} gibt

die nebenstehende Tabelle an:

Es gibt unendlich viele inäquivalente Lösungen für n=4 und k=2 oder 3. Wir haben sie in Kap.1 Abschnitt 4 bzw.5 kennengelernt in Gestalt der $\mathbf{U}_{\mathbf{x}}$, mit

$n \times k$	2	3	4	5	-6
2	1	1	Ø	_	ts.
3	1	1	1	Ø	_
4	00	00	1	1	Ø

 $x \in [0, \pi/z]$ und der v_x, v_yz , mit (x,y,z) aus einer geeigneten Teilmenge von $[0,2\pi)^3$.

Für alle n, für k=2 oder 3 und für beliebige Partitionen ist die Anzahl der Äquivalenzklassen immer größer gleich 1:

Für k=2 folgt dies aus der Existenz der Fouriermatrix F⇔ für alle n∈N. Sie ist eine VH-Matrix und damit eine VBH-Matrix mit beliebiger Partition. Für n, die keine Primzahl sind, konstruieren wir in Kapitel 5 sogar unendlich viele inäquivalente VH-Matrizen.

In Kap. 4 geben wir für alle n∈N zwei n×n VH-Matrizen mit Produkteigenschaft an und damit einen Repräsentanten für k=3 und wieder bel. Partition. Wir konstruieren dort für viele n auch Lösungen für größere k.

Vermutlich existieren aber bereits für n=6 keine drei VH-Matrizen mit Produkteigenschaften mehr : $A_{6.4}=9$??? (siehe Kapitel 5).

Für k > n+1 ist $A_{n,k}$ jeweils \varnothing , d.h. es gibt keine Lösungen mehr. Dies ist ein Spezialfall der Ungleichungen, die wir im nächsten Abschnitt beweisen.

3.2. EINE GEOMETRISCHE INTERPRETATION, SCHRANKEN

Mit M bezeichnen wir den n²-dimensionalen Vektorraum der komplexen n×n Matrizen. (Standard-) Inneres Produkt darauf ist:

$$\langle C | D \rangle = tr(C^*D) = \sum_{i=1}^{n} \sum_{j=1}^{n} (C_{i,j}^* d_{i,j})$$

Zur Einheitsmatrix orthogonal (d.h. mit obigem Inneren Produkt; der Kontext schließt Verwechslungen jeweils aus) sind genau jene Matrizen deren Spur gleich ∅ ist. Diese bilden einen (n²-1)-dimensionalen Teilraum von Mp, den wir mit Mp bezeichnen. Die orthogonale Projektion einer beliebigen Matrix A auf M° ist:

$$A \rightarrow A-(tr(A)/n)1$$

Das gestattet eine geometrische Interpretation des Problems, vorerst für orthog. Projektionsmatrizen:

$$\begin{array}{ll} & \text{tr}\left(PQ\right) &=& \frac{1}{n}\text{tr}\left(P\right)\text{tr}\left(Q\right) \\ \Leftrightarrow & \text{tr}\left(\left(P-\left(\text{tr}\left(P\right) \times n\right)\mathbf{1}\right)^{\#}\left(Q-\left(\text{tr}\left(Q\right) \times n\right)\mathbf{1}\right)\right) &=& \varnothing \end{array}$$

Also sind P und Q unabhängig bzgl. $\frac{1}{n}$ 1 genau dann, wenn sie orthogonal auf \mathbf{M}_{n}° projiziert zueinander orthogonal sind.

Sei jetzt $A = \sum_{i=1}^{r} a_i P_i$ eine selbstadj. Matrix, mit verschiedenen Eigenwerten: a_i , $4 \le i \le r$. Die assoz. Eigenraumprojektionen P_i , $4 \le i \le r$ sind paarweise orthogonal:

Also spannen sie einen r-dimensionalen Teilraum von M, auf. Wir bezeichnen diesen mit F(A), da: $f(A) = \sum_{i=1}^{r} f(a_i) P_i$

$$f(A) = \sum_{i=1}^{r} f(a_i) P_i$$

für komplexwertige Funktionen f gerade die Linearkombinationen der P, sind. Er kann auch als der Vektorraum der von A erzeugte (Matrizen-) Algebra interpretiert werden.

In F(A) liegt immer die Einheitsmatrix: $1 = \sum_{i=1}^{F} P_{i}$

Also ist:
$$F(A)^{\circ} := F(A) \cap M_n^{\circ}$$

nur noch ein (r-1)-dimensionaler Teilraum von M_p . Dieser wird von beliebigen r-1 der r Matrizen: $P_i - (\operatorname{tr} O_i) \times n) \mathbf{1}$, $1 \le i \le r$ aufgespannt.

3.4. LEMMA: Zwei komplexe, selbstadj. n×n Matrizen A und B sind unabhängig bzgl. $\frac{1}{n}$ 1 genau dann, wenn die Teilräume F(A)° und F(B)° zueinander orthogonal in M_n sind.

Bew.: A und B sind unabhängig bzgl. $\frac{4}{n}$ 1 genau dann, wenn es ihre Spektralprojektionen P_i und Ω_j jeweils sind. Also genau dann, wenn diese orthogonal projiziert auf M_n° zueinander jeweils orthogonal sind. Dies entspricht genau der Orthogonalität der von ihnen dort auf gespannten Teilräume $F(A)^\circ$ und $F(B)^\circ$.

Als wichtige Konsequenz folgen Ungleichungen:

3.5. SATZ: A_1, \ldots, A_k seien k paarweise bzgl. $\frac{1}{n}$ 1 unabhängige, selbstadjungierte Matrizen. A_i , $1 \le i \le k$ habe jeweils genau r_i verschiedene Eigenwerte.

i) Die Spektralprojektionen aller A_i , $1 \le i \le k$ zusammen spannen einen $(1 - k + \sum_{i=1}^k r_i) - \text{dimensionalen Teilraum von } M_n \text{ auf.}$

ii) also muß gelten:
$$(1 - k + \sum_{i=1}^{k} r_i) \le n^2$$
 (3.1)

iii) Kommutieren die $\mathbf{A}_{\mathbf{i}}$ paarweise, so muß mehr noch gelten:

$$(1 - k + \sum_{i=1}^{k} r_i) \leq n$$

Bew.: zu i): Die k jeweils (r_i-1) -dimensionalen Teilräume $F(A_i)^\circ$ von M_n sind paarweise zueinander orthogonal. Sie spannen zusammen also einen $\sum_{i=1}^k (r_i-1)$ – dimensionalen Teilraum auf. Dazu kommt noch die orthogonale Einheitsmatrix.

zu ii) und iii): Der Vektorraum M_n ist n²-dimensional. Kommutie – ⊅ende Matrizen spannen maximal einen n-dimensionalen Teilraum auf.≡

Vollständige Lösungen sind k paarweise bzgl. $\frac{1}{n}$ 1 unabhängige, selbstadjungierte Matrizen, für die ii) zur Gleichung wird. Kommutieren diese Matrizen und wird iii) zur Gleichung, so sprechen wir von vollständigen klassischen Lösungen.

Die Ungleichung iii) für kommutierende Matrizen, ist die bereits in der Einleitung angegebene Unglohg. (1.3) für bzgl. der Gleichverteilung unabhängige klassische Zufallsvariablen über einer nelementigen Menge. Als bekannte Spezialfälle führten wir die entsprechenden Schranken für paarw, orthog. Lat. Quadrate und für Orthogonale Anordnungen der Stärke zwei an.

Ein berühmtes Resultat, das bereits von Euler vermutet wurde, sagt, daß es keine zwei zueinander orthog. Lat. 6×6 Quadrate gibt. Eine parallele Vermutung für nichtkommutierende Matrizen ist A_{σ,4} =Ø. Wir schließen, daß es keine hinreichende Bedingung für die Existenz von Lösungen ist, falls eine der Ungleichungen erfüllt ist.

Betrachten wir wieder den Fall (nichtkommutierender), nichtentarteter \mathbf{A}_{i} , $\mathbf{1} \leq i \leq k$. Das heißt \mathbf{A}_{i} habe jeweils genau \mathbf{r}_{i} =n verschiedene Eigenwerte. Es folgt:

$$k \le n+1 \Rightarrow A_{n,k} = \emptyset \text{ für } k > n+1$$

Diese Schranke haben wir für kleine n bereits aus der Tabelle am Ende des vorigen Abschnitts herausgelesen. Im nächsten Kapitel zeigen wir $A_{n,n+1} \ge 1$ für Primzahlpotenzen $n=p^m$. Dies ist ein Spezialfall von folgendem:

Ang. n=q¹ für eine bel. Primzahlpotenz q und 1∈N. Die Matrizen sollen jeweils q verschiedene Eigenwerte haben. Dann folgt aus Globg. (3.1):

$$k \le (q^{2l}-1)/(q-1) = q^{2l-1}+q^{2l-2}+ \dots +q+1$$
 (3.2)

Wir konstruieren im nächsten Kapitel vollständige solche Lösungen.

Stellen wir zusätzlich die Forderung, daß die Matrizen paarweise kommutieren folgt aus (1.3):

$$k \le (q^{l}-1)/(q-1)$$

Solche vollständige Lösungen sind in Form von Orthogonalen Anordnungen bekannt (z.B. Raghavarao [36] §2.3). Für =2 entsprechen sie den bekannten, vollständigen Mengen paarweise orthog. Lateinischer q×q Quadrate. (Dénes(Keedwell [20] §5.2). Auch diese Ergebnisse folgen aus der Konstruktion in Kap.4.

3.3. TENSORPRODUKT

A sei eine m×n Matrix, B sei eine p×q Matrix. Das Tensorprodukt (oder direkte-, oder Kronecker-Produkt) von A und B ist eine mp×ng Matrix definiert durch:

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} \mathbf{a_{11}}^{\mathbf{B}} & \mathbf{a_{12}}^{\mathbf{B}} & \dots & \mathbf{a_{1n}}^{\mathbf{B}} \\ \mathbf{a_{21}}^{\mathbf{B}} & \mathbf{a_{22}}^{\mathbf{B}} & \dots & \mathbf{a_{2n}}^{\mathbf{B}} \\ \vdots & \vdots & & \vdots \\ \mathbf{a_{m1}}^{\mathbf{B}} & \mathbf{a_{m2}}^{\mathbf{B}} & \mathbf{a_{mn}}^{\mathbf{B}} \end{bmatrix}$$

Von den bekannten Rechenregeln sei besonders erinnert daran, daß für quadratische Matrizen ▲ und ß gilt:

$$tr(A\otimes B) = tr(A)tr(B)$$

Das Tensorprodukt eines Vektors $\mathbf{x} = (\mathbf{x_i}, \dots, \mathbf{x_n})^T \in \mathbb{C}^n$ und des Vektors $\mathbf{y} = (\mathbf{y_i}, \dots, \mathbf{y_m})^T \in \mathbb{C}^m$ ist $\mathbf{x} \otimes \mathbf{y} = (\mathbf{x_i} \mathbf{y^T}, \dots, \mathbf{x_n} \mathbf{y^T})^T \in \mathbb{C}^{mn}$. Es gilt mit n×n bzw. m×m Matrizen A und B: $(\mathbf{A} \otimes \mathbf{B}) (\mathbf{x} \otimes \mathbf{y}) = \mathbf{A} \mathbf{x} \otimes \mathbf{B} \mathbf{y}$.

Wir werden das Tensorprodukt in den nächsten zwei Kapiteln intensiv verwenden. Ein grundlegender Zusammenhang mit Unabhängigkeit bzgl. ½1 wurde bereits in der Einleitung skizziert:

3.6. SATZ: Kommutierende, selbstadjungierte n×n Matrizen A und B sind unabhängig bzgl. ½1 genau dann, wenn n=p.q für p,q∈N und es selbstadj. p×p bzw. q×q Matrizen Å und ß gibt, sodaß A und B zu den n×n Matrizen Å⊗1 und 1 oß (unitär) äquivalent sind.

Bew.: Daß Ã⊗1 q und 1 ⊗B (Index bei den Einheitsmatrizen bedeutet die Ordnung) für bel. selbstadj. p×p bzw. q×q Matrizen Å und B unabhängig bzgl. ½1 sind, folgt z.B. als Spezial all aus dem nächsten Lemma 3.7 (siehe auch Beispiel 2.12)

Kommutieren umgekehrt A und B, dann lassen sie sich mit einer unitären n×n Matrix V durch $A+A'=U^{-1}AU$ und $B+B'=U^{-1}BU$ gleichzeitig diagonalisieren.

Ihre Unabhängigkeit bzgl. $\frac{1}{n}$ 1 entspricht dann der von den Diagonal-einträgen, als klass. Zufallsvariablenüber einer n-elementigen Men-

ge Ω interpretiert, bzgl. der Gleichverteilung. In der Einleitung (Abschnitt 1.1) bewiesen wir, daß diese durch Umordnen der Punkte immer auf die Gestalt $\mathbf{f_A}(\omega_{ij}) = \mathbf{g_A}(i)$ und $\mathbf{f_B}(\omega_{ij}) = \mathbf{g_B}(j)$ gebracht werden können. (Glchg.(1.2), Indizes A und B bedeuten A bzw. B zugeordnet).

Mit unitären Permutationsmatrizen P kann durch $A' \rightarrow A'' = P^{-1}A'P$ und $B' \rightarrow B'' = P^{-1}B'P$ eine beliebige Anordnung der Diagonalpunkte erreicht werden. Ordnen wir sie als $(\omega_{i1}, \ldots, \omega_{iq}, \omega_{21}, \ldots, \omega_{2q}, \ldots, \omega_{p1}, \ldots, \omega_{pq})$ der Reihe nach an. Dann ist $A'' = \tilde{A} \otimes 1_q$ mit der diagonalen p×p Matrix $\tilde{A} = \text{diag}(g_{A}(\omega), \ldots, g_{A}(p))$ und $B'' = 1_p \otimes \tilde{B}$ mit der diagonalen q×q Matrix $\tilde{B} = \text{diag}(g_{B}(\omega), \ldots, g_{B}(q))$.

3.7. LEMMA: A und B seien bzgl. $\frac{1}{n}$ 1 unabhängige n×n Matrizen, C und D seien bzgl. $\frac{1}{m}$ 1 unabhängige m×m Matrizen. Dann sind die mn×mn Matrizen A⊗C und B⊗D unabhängig bzgl. $\frac{1}{mp}$ 1.

Bew.: Seien die Spektralzerlegungen:

$$\mathbf{A} = \sum_{i=1}^r \mathbf{a}_i \mathbf{P}_i \text{ , } \mathbf{B} = \sum_{j=1}^s \mathbf{b}_j \mathbf{Q}_j \text{ , } \mathbf{C} = \sum_{k=1}^p \mathbf{c}_k \mathbf{M}_k \text{ , und } \mathbf{D} = \sum_{l=1}^q \mathbf{d}_l \mathbf{N}_l$$

mit jeweils verschieden Eigenwerten a_i , b_j , c_k , d_l und jeweils assozierten Projektionen auf die Eigenräume P_i , Q_j , M_k und N_l . Es folgt:

$$A \otimes C = \sum_{i=1}^{r} \sum_{k=1}^{p} a_{i} C_{k} (P_{i} \otimes M_{k}) , \qquad B \otimes D = \sum_{j=1}^{s} \sum_{l=1}^{q} b_{j} d_{l} (Q_{j} \otimes N_{l})$$

Nehmen wir vorerst an die Eigenwerte $a_i c_k$, $1 \le i \le r$, $1 \le k \le p$ bzw. $b_j d_l$, $1 \le j \le s$, $1 \le l \le q$ von A⊗C bzw. B⊗D sind jeweils verschieden. Ihre assoz. Projektionen $P_i \otimes M_k$ bzw. $Q_i \otimes N_l$ erfüllen für alle i,j,k,l:

$$\operatorname{tr}\left((P_{i}\otimes M_{k})\;(Q_{j}\otimes N_{l})\right)\;=\;\operatorname{tr}\left((P_{i}Q_{j})\otimes (M_{k}N_{l})\right)\;=\;\operatorname{tr}\left(P_{i}Q_{j}\right)\operatorname{tr}(M_{k}N_{l})\;=\;$$

unter Verwendung der Unabhängigkeit von A und B bzw. C und D folgt

$$= \frac{\mathbf{i}}{n} \text{tr}(\mathbf{P}_i) \text{tr}(\mathbf{Q}_j) \frac{\mathbf{i}}{m} \text{tr}(\mathbf{M}_k) \text{tr}(\mathbf{N}_l) = \frac{\mathbf{i}}{mn} \text{tr}(\mathbf{P}_i \otimes \mathbf{M}_k) \text{tr}(\mathbf{Q}_j \otimes \mathbf{N}_l)$$

Sind die Eigenwerte a_ic_k bzw. b_jd_i nicht jeweils alle verschieden, so sind die Proj. auf die Eigenräume von $A\otimes C$ bzw. $C\otimes D$ zu verschiedenen Eigenwerte jeweils Summen der $P_i\otimes M_k$ bzw. $Q_j\otimes N_k$. Mithilfe von Prop. 2.4 folgt auch dann die Unabhängigkeit von $A\otimes C$ und $B\otimes D$ bzgl. $\frac{1}{nm}1$.

In Kap. 5 verallgemeinern wir Lemma 3.7 und übertragen es in die Sprache der zugeordneten VBH-Matrizen. Das ergibt ein nützliches Konstruktionsprinzip für solche Matrizen. Im nächsten Kapitel findet eine einfache Folgerung Anwendung:

3.8. Korollar: Angenommen A_1, \ldots, A_k sind k paarweise bzgl. $\frac{1}{n}$ 1 unabhängige n×n Matrizen und B_1, \ldots, B_k sind k paarweise bzgl. $\frac{1}{m}$ 1 unabhängige m×m Matrizen. Dann sind $A_1 \otimes B_1, \ldots, A_k \otimes B_k$ k paarweise bzgl. $\frac{1}{n}$ 1 unabhängige mn×mn Matrizen.

Kommutieren die A_i , $1 \le i \le k$ und die B_j , $1 \le j \le k$ jeweils paarweise, dann tun dies auch die $A_i \otimes B_i$, $1 \le i \le k$.

Angenommen \mathbf{A}_i hat \mathbf{r}_i verschiedene Eigenwerte und \mathbf{B}_i hat \mathbf{l}_i verschiedene Eigenwerte. Bei geeigneter Wahl dieser Eigenwerte (die ja aufgrund der Äquivalenzklassenbildung beliebig verändert werden können), sodaß ihr Produkte jeweils verschieden sind, hat $\mathbf{A}_i \otimes \mathbf{B}_i$ genau $\mathbf{r}_i \mathbf{l}_i$ verschiedene Eigenwerte. Die Eigenraumdimensionen sind dann jeweils genau die Produkte der von \mathbf{A}_i und \mathbf{B}_i .

Es ist leicht zu sehen, daß dies, speziell auf das Problem orthogonaler Lateinischer Quadrate angewandt, der Idee des Satzes von Mac Neish entspricht (siehe Dénes/Keedwell [20], p.390).

4. VOLLSTÄNDIGE SYSTEME

Im ersten Abschnitt werden die Weylmatrizen, deren Tensorprodukte, sowie einige Fakten aus der Theorie endlicher Körper vorgestellt. Sie bilden die Hilfsmittel für den zweiten Abschnitt, in dem wir für beliebige Primzahlpotenzen g=p[™] und beliebige t∈N die Existenz von $(q^{2l}-1)/(q-1)$ selbstadj. Matrizen der Ordnung $n=q^{l}$ mit jeweils q verschiedenen Eigenwerten zeigen, die paarweise bzgl. 11 unabhängig sind. Diese vollständigen Lösungen enthalten bekannte vollständige, klassische Lösungen als Teilmengen. Im dritten Abschnitt wird für ungerade a speziell eine Formel für a VH-Matrizen der Ordnung a mit Produkteigenschaft abgeleitet.

4.1 WEYLMATRIZEN, ENDLICHE KÖRPER

Sei $\lambda = e^{i2\pi/n}$. Zwei unitäre n×n Matrizen sind:

$$\mathbf{V} = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{bmatrix} \qquad \mathbf{U} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & 0_{2} & \dots & 0 \\ 0 & 0 & \lambda^{2} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda^{n-4} \end{bmatrix}$$

Es folgt leicht:

$$V^{n} = U^{n} = 1$$
 $VU = \lambda UV$

und durch Iteration:
$$V^rU^s = \lambda^{rs}U^sV^r$$

für alle r.s∈Z

Es seien:

$$W(r,s) := V^r U^s \tag{4.1}$$

Für O≤r.s≤n-1 sind das n² verschiedene sogenannte Weylmatrizen. Bel. r,s ∈ Z eingesetzt liefern modulo n dieselben Matrizen. Als Einträge r,s können also auch die Elemente von $\mathbb{Z}_{n} = \mathbb{Z}/n\mathbb{Z}$ (repräsentiert z.B. durch 0,1,...,n-1) genommen werden. Damit folgt:

$$W(r,s)W(r',s') = \lambda^{-r's}W(r+r',s+s')$$
 (4.2)

für beliebige r,r',s,s'∈ Z,.

Die Zuordnung $(r,s) \in \mathbb{Z}_n \times \mathbb{Z}_n \to W(r,s)$ liefert die eindeutige irreduzible und treue Strahldarstellung der abelschen 2n-elementigen, additiven Gruppe $\mathbb{Z}_n \times \mathbb{Z}_n$ (Weyl [48], Kap.4, §15).

Die n⁹ Matrizen λ^q $\mathbf{W}(\mathbf{r},\mathbf{s})$, mit $\mathbf{q}_{r,\mathbf{s}} \in \mathbb{Z}_n$ bilden eine gewöhnliche, irreduzible und treue Darstellung der (nichtabelschen) sogenannten Heisenberggruppe (siehe Auslander/Tolimieri [04], p.20).

Seien r,s ∈ Z_p. Es ist leicht zu sehen, daß:

$$tr(\mathbf{W}(r,s)) = \begin{cases} n & \text{für } r=s=0 \\ 0 & \text{sonst} \end{cases}$$
 (4.3)

sowie:

$$W^{-1}(r,s) = W^{*}(r,s) = \lambda^{-rs} W(-r,-s)$$

woraus insgesamt folgt:

$$\langle \mathbf{W}(\mathbf{r},\mathbf{s}) | \mathbf{W}(\mathbf{r}',\mathbf{s}') \rangle := \operatorname{tr} \left(\mathbf{W}^*(\mathbf{r},\mathbf{s}) \mathbf{W}(\mathbf{r}',\mathbf{s}') \right) = \begin{cases} n & \text{für } \mathbf{r} = \mathbf{r}', \mathbf{s} = \mathbf{s}' \\ \emptyset & \text{sonst} \end{cases}$$
(4.4)

Die n^2 Matrizen W(r,s) sind also bzgl. des Standard-Inneren Produktes (siehe Kap.3, Abschn.2) auf M_n paarweise orthogonal. Die Matrizen $\sqrt{n}W(r,s)$, $r,s \in \mathbb{Z}_n$ bilden eine orthonormierte Basis von M_n . (siehe auch Schwinger [38]).

Das Gegenstück der n×n Matrizen $\mathbf{W}(\mathbf{r},\mathbf{s})$ für n= ∞ sind die Operatoren von Glchg.(2.11), die eine irreduzible Strahldarstellung der zweiparametrige, abelschen, additiven Lie-Gruppe $\mathbb{R}\times\mathbb{R}$ bilden. (Siehe auch Weyl [48], Kap.4, §15) In Kapitel 2, Abschn.3 zeigten wir, daß die Menge der kontinuierlichen Weyloperatoren (2.11) in unendlich viele einparametrige Untergruppen $\mathbf{U}_{\alpha}(t)$ zerlegt werden kann, (die nur die Einheitsmatrix paarweise gemeinsam haben), mit jeweils einem selbstadjungierten Generator \mathbf{A}_{α} . Prop. 2.14 zeigt deren paarweise Unabhän gigkeit bzgl. 1.

Es liegt nahe auch für den diskreten Fall zu versuchen die $\mathbf{W}(\mathbf{r},\mathbf{s})$, $\mathbf{r},\mathbf{s} \in \mathbb{Z}_n$ in Untergruppen, zumindest aber Teilmengen kommutierender Matrizen vollständig zu zerlegen, sodaß sich diese jeweils nur in der Einheitsmatrix paarweise überschneiden. Aus Glohg. (4.2) folgt, daß $\mathbf{W}(\mathbf{r},\mathbf{s})$ und $\mathbf{W}(\mathbf{r}',\mathbf{s}')$ kommutieren, genau dann, wenn in \mathbb{Z}_n , d.h.

modulo n gerechnet, gilt:

$$rs' = sr'$$
 (4.5)

Sei z.B. n=p...Primzahl. Wir identifizieren (r,s), r,s $\in \mathbb{Z}_p$ mit Elementen von \mathbb{Z}_p^2 , dem zweidimensionalen Vektorraum über dem Körper \mathbb{Z}_p . (4.5) ist genau die Bedingung, daß (r,s) und (r',s') in einem gemeinsamen, eindimensionalen Teilraum von \mathbb{Z}_p^2 liegen. Es gibt p+1 eindim. Teilräume von \mathbb{Z}_p^2 mit jeweils p Punkten darin, die sich nur im Nullpunkt (0,0) überschneiden. Das ist also eine passende Zerlegung für n=p.

Für nichtprime n sind nur unvollständige solche, bis auf den Nullpunkt disjunkte Zerlegungen möglich, auf die wir in Abschnitt 4 zu sprechen kommen.

4.1 BEISPIEL: Für n=2 ist all dies einfach:

$$\mathbf{W}(0,0) = \mathbf{1}$$
 $\mathbf{W}(1,0) = \mathbf{V} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $\mathbf{W}(0,1) = \mathbf{U} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $\mathbf{W}(1,1) = \mathbf{V}\mathbf{U} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

Die Zerlegung in die drei Teilmengen ist: $(1, \mathbf{W}(1,0))$, $(1, \mathbf{W}(0,1))$, $(1, \mathbf{W}(1,1))$. Es ist auch leicht direkt nachzuprüfen, daß bereits $\sigma_{\mathbf{x}} = \mathbf{W}(1,0)$, $\sigma_{\mathbf{y}} = i\mathbf{W}(1,1)$ und $\sigma_{\mathbf{z}} = \mathbf{W}(0,1)$ drei paarweise bzgl. $\frac{1}{2}\mathbf{1}$ unabhängige, selbstadj., nichtentartete Matrizen sind (mit jeweils den zwei Eigenwerten ±1). Diese Matrizen heißen Pauli-Spinmatrizen. (Thirring [43],Bd.3, p.31). Zwei zugeordnete VH-Matrizen sind:

$$\mathbf{U_0} = \sqrt{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$
 und $\mathbf{U_1} = \sqrt{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

 $\mathbf{U_o^{-1}} \sigma_{\mathbf{x}} \mathbf{U_o} = \sigma_{\mathbf{z}}, \ \mathbf{U_1^{-1}} \sigma_{\mathbf{y}} \mathbf{U_1} = \sigma_{\mathbf{z}}.$ Dies ist die eindeutige (Kap.3-Äquiv.) und einzige vollständige Lösung für n=2.

Für p>2 liegt es nahe für jede der p+1 Mengen eine selbstadj. Matrix zu suchen, die eine Linearkombination der p Matrizen der Menge ist. (Der Übergang zu infinitesimalen Erzeugenden, wie im Unendlichdimensionalen, ist ja nicht möglich).

Wir führen die Konstruktion aber gleich allgemeiner durch, indem wir bemerken, daß der oben beschriebene Ansatz daran anknüpfte, daß \mathbb{Z}_p ein Körper ist. Es bietet sich also an, zu versuchen ihn unter Verwendung der Theorie beliebiger endlicher Körper auf bel. Primzahlpotenzen: p^k , kel auszudehnen. Dafür müssen Tensorprodukte von Weylmatrizen herangezogen werden.

r und s seien zwei k-tupel von Elementen r_i bzw. $s_i \in \mathbb{Z}_p$, $1 \le i \le k$:

$$r = (r_1, \dots, r_k)$$
 $s = (s_1, \dots, s_k)$

Für alle i≤i≤k seien **W**(r_i,s_i) jeweils p×p Weylmatrizen. p ist im folgenden immer eine Primzahl. Durch:

$$\mathbf{Z}(\mathbf{r},\mathbf{s}) := \mathbf{W}(\mathbf{r}_{i},\mathbf{s}_{i}) \otimes \ldots \otimes \mathbf{W}(\mathbf{r}_{k},\mathbf{s}_{k})$$
 (4.6)

werden n^2 $(n=p^k)$ verschieden n×n Matrizen definiert. Aus (4,2) folgt:

$$Z(r,s)Z(r',s') = \lambda^{-\langle r' \mid s \rangle} Z(r+r',s+s')$$
 (4.7)

Dabei ist das innere Produkt:

$$\langle r | s \rangle = r_4 s_4 + \dots + r_k s_k$$

und die Addition punktweise:

$$r+s = (r_i+s_i, \dots, r_k+s_k)$$

Es wird immer in \mathbb{Z}_{p} gerechnet, d.h. modulo p.

Es folgt sofort, daß $\mathbf{Z}(\mathbf{r},\mathbf{s})$ und $\mathbf{Z}(\mathbf{r}',\mathbf{s}')$ kommutieren, genau dann wenn in \mathbb{Z}_p gilt: $\langle \mathbf{r} | \mathbf{s}' \rangle = \langle \mathbf{r}' | \mathbf{s} \rangle$ (4.8)

(4.3) wird zu:

$$tr(\mathbf{Z}(\mathbf{r},\mathbf{s})) = \begin{cases} n & \text{für } r_i = s_i = \emptyset, \text{ für alle } 1 \le i \le k \\ \emptyset & \text{sonst} \end{cases}$$
 (4.9)

(4.4) wird zu:

$$\langle Z(r,s) | Z(r',s') \rangle =$$

$$= \operatorname{tr} \left(\mathbf{Z}^{*}(\mathbf{r}, \mathbf{s}) \mathbf{Z}(\mathbf{r}', \mathbf{s}') \right) = \begin{cases} n & \text{für } r_{i} = r'_{i}, \ s_{i} = s'_{i}, \ \text{für alle } 4 \le i \le k \\ \emptyset & \text{sonst} \end{cases}$$
(4.10)

Die n² verschiedenen n×n Matrizen Z(r,s) sind also auch orthogonal. Sie bilden eine Strahldarstellung der elementaren abelschen Gruppe EA(p²k) der Ordnung p²k. Elementare abelsche Gruppen sind isomorph zu endlichen Körpern F, als additive Gruppen interpretiert. Die genaue Beschreibung der Zuordnung benötigt Vorbereitung.

Wir erinnern an einige Elemente der Theorie endlicher Körper. Als Standardreferenz hierfür sei nachdrücklich auf Lidl/Niederreiter [31] hingewiesen. Folgendes findet sich in Kap.2,§3.

F sei der endliche Körper der Ordnung q^m , mit dem Subkörper K der Ordnung $q=p^a$. F kann als m-dimensionaler Vektorraum über K interpretiert werden. Eine Basis von F über K heißen m geordnete Elemente $\alpha=(\alpha_1,\ldots,\alpha_m)$ von F, falls jedes Element $r \in F$ eindeutig in folgender Form dargestellt werden kann:

$$r = r_1 \alpha_1 + ... + r_m \alpha_m$$
 mit $r_i \in K$, für alle $1 \le i \le m$

Sei mit $\mathbf{r}_{\alpha} = (\mathbf{r}_{1}, \dots, \mathbf{r}_{m})$ das m-tupel der Koeffizienten von $\mathbf{r} \in \mathbf{F}$ bzgl. der Basis α bezeichnet.

Die Spur Tr_{F/K}(a) eine Elementes a∈F über K ist definiert durch:

$$\mathsf{Tr}_{\mathbf{F}/\mathbf{K}}(\mathbf{a}) = \mathbf{a} + \mathbf{a}^{\mathbf{q}} + \ldots + \mathbf{a}^{\mathbf{q}^{m-1}}$$

Ist K der Primsubkörper von F, dann wird $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\mathbf{a})$ als absolute Spur von \mathbf{a} bezeichnet und einfach als $\mathrm{Tr}(\mathbf{a})$ angeschrieben.

Die Spur ist eine lineare Abbildung von F in K:

$$\operatorname{Tr}_{F/K}(a+b) = \operatorname{Tr}_{F/K}(a) + \operatorname{Tr}_{F/K}(b)$$
 für alle $a,b \in F$
$$\operatorname{Tr}_{F/K}(ca) = \operatorname{cTr}_{F/K}(a)$$
 für alle $c \in K$, $a \in F$

Sie ist transitiv, d.h. sei F Subkörper des endlichen Körpers E, so gilt: $Tr_{E/K}(a) = Tr_{F/K}(Tr_{E/F}(a))$ für alle $a \in E$ (4.11)

Zwei Basen $\alpha = (\alpha_1, \dots, \alpha_m)$ und $\beta = (\beta_1, \dots, \beta_m)$ von F über K heißen dual, falls für alle $1 \le i,j \le m$ gilt:

$$\operatorname{Tr}_{\mathbf{F} \times \mathbf{K}}(\alpha_{\mathbf{i}} \beta_{\mathbf{j}}) = \begin{cases} 1 & \text{für } \mathbf{i} = \mathbf{j} \\ \emptyset & \text{für } \mathbf{i} \neq \mathbf{j} \end{cases}$$

Zu jeder beliebigen Basis existiert eine eindeutige duale Basis.

Sei Fⁿ der n-dimensionale Vektorraum über dem endl. Körper F der Ordnung q. Einfaches Abzählen zeigt, daß es

$$[n]_{q} := \frac{q^{n-1}}{q-1} = q^{n-1} + q^{n-2} + \dots + q+1$$
 (4.12)

verschiedene eindimensionale Teilräume von \mathbf{F}^n gibt, mit jeweils q Punkten darin. Abgesehen vom Nullpunkt, wo sich alle Teilräume überschneiden bilden sie eine disjunkte Zerlegung von \mathbf{F}^n . Speziell gibt es q+1 eindim. Teilräume von \mathbf{F}^2 . 4.2. LEMMA: $(\alpha_1, \ldots, \alpha_m)$ und $(\beta_1, \ldots, \beta_m)$ seien duale Basen von F über K.

i) Sei $r=r_1\alpha_1+...+r_m\alpha_m$ und $s=s_1\beta_1+...+s_m\beta_m$ mit r_i , $s_i\in K$, dann folgt:

$$\mathsf{Tr}_{\mathbf{F}/\mathbf{K}}(\mathbf{r}\mathbf{s}) = \mathsf{r}_{\mathbf{i}}\mathsf{s}_{\mathbf{i}}^{+}\dots+\mathsf{r}_{\mathsf{m}}\mathsf{s}_{\mathsf{m}}^{-} = : \langle \mathsf{r}_{\alpha}|\mathsf{s}_{\beta}\rangle \tag{4.13}$$

ii) Seien (r,s) und (r',s') aus demselben eindimensionalen Teilraum von F^2 , so gilt in K: $\langle r_{\alpha}|s_{\beta}'\rangle = \langle r_{\alpha}'|s_{\beta}\rangle$.

Bew.: i)
$$\mathsf{Tr}_{\mathbf{F}/\mathbf{K}}(\mathbf{r}\mathbf{s}) = \sum_{i=1}^{m} \sum_{j=1}^{m} r_{i} s_{j} \mathsf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_{i} \beta_{j}) = \sum_{i=1}^{m} r_{i} s_{i}$$

ii) Liegen (r,s) und (r',s') im selben eindim. Teilraum von F^2 , so ist in F: $rs'-r's=\emptyset$

also:
$$\text{Tr}_{\mathbf{F}/\mathbf{K}}(\mathbf{r}\mathbf{s}'-\mathbf{r}'\mathbf{s}) = \emptyset \quad \Leftrightarrow \quad \text{Tr}_{\mathbf{F}/\mathbf{K}}(\mathbf{r}\mathbf{s}') = \text{Tr}_{\mathbf{F}/\mathbf{K}}(\mathbf{r}'\mathbf{s})$$

und das entspricht mit i) genau der Folgerung.

Zuletzt benötigen wir noch additive Charaktere (siehe Lidl/Niederreiter [31] Kap.5,\$1). Ein additiver Charakter \varkappa des endl. Körpers $\mathbf{F_q}$ der Ordnung $\mathbf{q=p}^m$ ist eine Abbildung von $\mathbf{F_q}$ in die komplexen Zahlen mit Absolutbetrag 1, sodaß gilt:

$$\chi(a+b) = \chi(a)\chi(b)$$
 für alle a,b \in F_q

Das sind eindimensionale Darstellungen von $\mathbf{F_q}$ als additive Gruppe. Ein kanonischer additiver Charakter läßt sich mithilfe der absoluten Spur: Tr von $\mathbf{F_q}$ über seinem Primkörper $\mathbf{F_p}$ definieren, indem wir $\mathbf{F_p}$ mit $\mathbf{Z_p}$ identifizieren:

$$\chi_{\mathbf{i}}(\mathbf{a}) := e^{2\pi i \mathbf{Tr}(\mathbf{a})/p}$$
 für alle $\mathbf{a} \in \mathbf{F}_{\mathbf{q}}$ (4.14)

Für Jedes bel. c∈F ergibt sich ein weiterer Charakter durch:

$$\chi_{c}(a) := \chi_{a}(ca)$$
 für alle $a \in F_{a}$

Diese q verschiedenen Charaktere χ_c , $c \in \mathbb{F}_q$ sind alle die es gibt, inklusive dem trivialen Charakter $\chi_o(a) = 1$ für alle $a \in \mathbb{F} = \mathbb{F}_q$. Für nichttriviale Charaktere gilt:

$$\sum_{\mathbf{a} \in F} \chi_{\mathbf{c}}(\mathbf{a}) = \emptyset \quad \text{für } c \neq \emptyset$$

Daraus folgt die bekannte (erste) Orthogonalitätsrelation:

$$\frac{1}{q} \sum_{\mathbf{a} \in \mathbf{F}} \bar{\chi}_{\mathbf{c}}(\mathbf{a}) \chi_{\mathbf{d}}(\mathbf{a}) = \begin{cases} 1 & \text{für c=d} \\ \emptyset & \text{für c\neq d} \end{cases}$$
 (4.15)

Der Strich bedeutet komplexe Konjugation.

4.2. VOLLSTÄNDIGE LÖSUNGEN

 $\alpha=(\alpha_1,\dots,\alpha_m)$ und $\beta=(\beta_1,\dots,\beta_m)$ seien duale Basen des endlichen Körpers F_q der Ordnung $q=p^m$ über dem Primsubkörper F_p . Sei F_p mit \mathbb{Z}_p identifiziert. Dann ist durch

$$r \leftrightarrow r_{\alpha} = (r_{i}, \dots, r_{m})$$
 und $s \leftrightarrow s_{\beta} = (s_{i}, \dots, s_{m})$

jeweils eine ein-eindeutige Zuordnung von Elementen r bzw. s aus $\mathbf{F_q}$ zu m-tupeln von Elementen aus \mathbb{Z}_p gegeben. Und damit ist durch

$$(r,s) \leftrightarrow Z(r_{\alpha},s_{\beta})$$
 für bel. $r,s\in F_q$ (4.16)

eine ein-eindeutige Zuordnung der Elemente $(r,s) \in \mathbb{F}_q^2$ zu den q^2 verschiedenen $q \times q$ Matrizen $\mathbf{Z}(r,s)$ (siehe Glchg.(4.6)) gegeben.

4.3. Lemma: Sind (r,s) und (r',s') aus demselben eindimensionalen Teilraum von F_q^2 , dann kommutieren $Z(r_\alpha,s_\beta)$ und $Z(r'_\alpha,s'_\beta)$.

Bew.: Nach Lemma 4.2.ii) folgt aus der Vorraussetzung, daß in \mathbb{Z}_p : $\langle \mathbf{r}_{\alpha} | \mathbf{s}_{\beta} \rangle = \langle \mathbf{r}_{\alpha}' | \mathbf{s}_{\beta} \rangle$

und das ist nach Globg. (4.8) äquivalent zur Folgerung.

Sei L ein bel. eindimensionaler Teilraum von F_q^z und mit $\mathbf{Z}(\mathbf{L})$ die Menge der den q Punkten (\mathbf{r},\mathbf{s}) L zugeordneten q Matrizen $\mathbf{Z}(\mathbf{r}_{\alpha},\mathbf{s}_{\beta})$ bezeichnet. Mit $\mathbf{\bar{Z}}(\mathbf{L})$ sei die Menge der komplexen Linearkombinationen der Matrizen aus $\mathbf{Z}(\mathbf{L})$ bezeichnet. $\mathbf{\bar{Z}}(\mathbf{L})$ ist ein linearer Teilraum von \mathbf{M}_q , dem Vektoraum der komplexen q×q Matrizen.

4.4. LEMMA: In jedem $\overline{Z}(L)$ liest eine nichtentartete, selbstadj. Matrix A_L und $\overline{Z}(L) = F(A_L) = \{f(A_L): f: \mathbb{R} \to \mathbb{C}\}$, A_L ist bis auf die Wahl der Eigenwerte eindeutig festgelegt.

Bew.: Seien die 9 paarweise kommutierenden, normalen Matrizen in $\mathbf{Z}(\mathbf{L})$ gleichzeitig diagonalisiert. Nach Glchg.(4.10) sind sie paarweise orthogonal. Sie bilden also eine Basis für den 9-dimensionalen Vektorraum der Diagonalmatrizen. Als Linearkombination enthalten sie also insbesondere eine Diagonalmatrix mit 9 verschiedenen, reellen Diagonaleinträgen, d.h. rücktransformiert eine nichtentartete und selbstadj. Matrix $\mathbf{A}_{\mathbf{L}}$. $\mathbf{Z}(\mathbf{L}) = \mathbf{F}(\mathbf{A}_{\mathbf{L}})$ folgt durch Dimensionsvergleich.

4.5. SATZ: $q=p^m$ sei eine Primzahlpotenz. Die q+1 verschiedenen $q\times q$ Matrizen A_L bilden eine vollständige Menge paarweise bzgl. $\frac{1}{q}$ 1 unabhängiger, selbstadjungierter, nichtentarteter Matrizen.

Bew.: Der q-1 dimensionale Teilraum $F(A_L)^\circ$ von M_q , aller Matrizen mit Spur Ø aus $F(A_L)=\overline{Z}(L)$, wird nach Glohg.(4.9) durch die q-1 Matrizen in $Z(L)/\{1\}$ aufgespannt. Für $L\not=L'$ sind diese Mengen disjunkt und also nach Glohg.(4.10) die Matrizen darin paarweise orthogonal auf M_q . Also sind $F(A_L)^\circ$ und $F(A_L)^\circ$ für $L\not=L'$ orthogonal. Nach Lemma 3.4 sind folglich A_L und A_L , unabhängig bzgl. $\frac{1}{q}$ 1.

Dies ist das angekündigte Resultat A_{n,n+1}≥1 für n=p^m; siehe auch Tabelle; Seite 36. Zum letzten Eintrag dort zeigen wir ein Bsp.:

4.6. BEISPIEL: Sei q=4. c sei eine Wurzel des irreduziblen Polynoms x²+x+1 vom Grad 2 über F_2 . Jedes Element r aus F_4 ist eindeutig darstellbar als $r=r_4+r_2$ c mit r_4 , $r_2 \in F_2$. (Rechnen in dieser Darstellung ist definiert durch punktweise Addition und Reduktion der Potenzen von c entsprechen $c^2=c+1$ bei Multiplikation.) Zur Basis $\alpha_4=1$ und $\alpha_2=c$ dual ist die Basis $\beta_4=1+c$ und $\beta_2=1$. Sei $s=s_4(1+c)+s_2$ mit $s_4,s_2\in F_2$. Den fünf eindim. Teilräumen von F_4^2 ; $S=\{(o,s): s\in F_4\}$ und $T_a=\{(r,ar): r\in F_4\}$, $a\in F_4$ sind je vier $\mathbf{Z}(r_\alpha,s_\beta)=\mathbf{W}(r_4,s_4)\otimes\mathbf{W}(r_2,s_2)$ zugeordnet:

```
\begin{split} Z(S) &= \left\{1, \, 1 \otimes \mathsf{W}(0,1), \, \mathsf{W}(0,1) \otimes 1, \, \mathsf{W}(0,1) \otimes \mathsf{W}(0,1)\right\} \\ Z(T_{_{\mathbf{O}}}) &= \left\{1, \, 1 \otimes \mathsf{W}(1,0), \, \mathsf{W}(1,0) \otimes 1, \, \mathsf{W}(1,0) \otimes \mathsf{W}(1,0)\right\} \\ Z(T_{_{\mathbf{I}}}) &= \left\{1, \, \mathsf{W}(0,1) \otimes \mathsf{W}(1,1), \, \mathsf{W}(1,0) \otimes \mathsf{W}(0,1), \, \mathsf{W}(1,1) \otimes \mathsf{W}(1,0)\right\} \\ Z(T_{_{\mathbf{C}}}) &= \left\{1, \, \mathsf{W}(0,1) \otimes \mathsf{W}(1,0), \, \mathsf{W}(1,1) \otimes \mathsf{W}(0,1), \, \mathsf{W}(1,0) \otimes \mathsf{W}(1,1)\right\} \\ Z(T_{_{\mathbf{I}+\mathbf{C}}}) &= \left\{1, \, 1 \otimes \mathsf{W}(1,1), \, \mathsf{W}(1,1) \otimes 1, \, \mathsf{W}(1,1) \otimes \mathsf{W}(1,1)\right\} \end{split}
```

Die 2×2 Matrizen W(r,s) von Beispiel 5.1 eingesetzt ergibt explizit:

$$Z(S) = \left\{ \mathbf{i}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1$$

Die Matrizen jeder dieser Mengen kommutieren paarweise. Als Linear-kombination der Matrizen aus $\mathbf{Z}(S)$ erhalten wir z.B. jede bel. Diagonalmatrix und als $\mathbf{A_L}$ für $\mathbf{L} = \mathbf{S}$ wird eine nichtenartete solche gewählt. Ebenso kann leicht zu jedem $\mathbf{L} = \mathbf{T_a}$, $\mathbf{a} \in \mathbf{F_4}$ eine nichtentartete, selbstadjungierte Matrix $\mathbf{A_L} \in \mathbf{\overline{Z}}(\mathbf{L})$ gebildet werden.

Wir bilden für alle $\mathbf{a} \in \mathbf{F_4}$ unitäre Matrizen $\mathbf{U_a}$, die jeweils alle Matrizen aus $\mathbf{Z}(\mathbf{T_a})$ gleichzeitig diagonalisieren:

Für $\mathbf{A_L} \in \mathbf{Z}(\mathbf{T_a})$, $\mathbf{a} \in \mathbf{F_4}$ gilt dann, daß $\mathbf{U_a}^{-1} \mathbf{A_L} \mathbf{U_a}$ eine Diagonalmatrix ist. Das heißt die $\mathbf{U_a}$, $\mathbf{a} \in \mathbf{F_4}$ sind vier zugeordnete VH-Matrizen. Ihre Produkteigenschaft läßt sich auch leicht explizit nachprüfen.

Die Konstruktion, die zu Satz 4.5 führte, erlaubt eine geradlinige Verallgemeinerung: Sei:

$$\bar{\mathbf{r}} = (\mathbf{r}^{(1)}, \dots, \mathbf{r}^{(l)})$$
 und $\bar{\mathbf{s}} = (\mathbf{s}^{(1)}, \dots, \mathbf{s}^{(l)})$

mit $\mathbf{r}^{(i)}, \mathbf{s}^{(i)} \in \mathbf{F}_q$, für alle $\mathbf{1} \le \mathbf{i} \le \mathbf{1}$. $(\bar{\mathbf{r}}, \bar{\mathbf{s}}) = (\mathbf{r}^{(i)}, \dots, \mathbf{r}^{(l)}, \mathbf{s}^{(l)}, \dots, \mathbf{s}^{(l)})$ sei als Elemente von \mathbf{F}_q^{2l} interpretiert. Durch:

$$(\bar{\mathbf{r}}, \bar{\mathbf{s}}) \leftrightarrow Z(\bar{\mathbf{r}}, \bar{\mathbf{s}}) := Z(\mathbf{r}_{\alpha}^{(1)}, \mathbf{s}_{\beta}^{(1)}) \otimes \ldots \otimes Z(\mathbf{r}_{\alpha}^{(1)}, \mathbf{s}_{\beta}^{(1)})$$
 (4.17)

erhalten wir eine ein-eindeutige Zuordnung der q^{2l} Elemente von F_q^{2l} zu den $q^l \times q^l$ Matrizen $Z(\bar{r}, \bar{s})$. Diese sind ml-fache Tensorprodukte von pxp Weylmatrizen (Globa, (4.6)).

4.7. Lemma: Sind $(\bar{\mathbf{r}},\bar{\mathbf{s}})$ und $(\bar{\mathbf{u}},\bar{\mathbf{v}})$ aus demselben eindimensionalen Teilraum von $\mathbf{F}_{\mathbf{q}}^{2l}$, dann kommutieren $\mathbf{Z}(\bar{\mathbf{r}},\bar{\mathbf{s}})$ und $\mathbf{Z}(\bar{\mathbf{u}},\bar{\mathbf{v}})$.

Bew.: Sind $(\bar{\mathbf{r}},\bar{\mathbf{s}})=(\mathbf{r}^{(1)},\ldots,\mathbf{r}^{(1)},\mathbf{s}^{(1)},\ldots,\mathbf{s}^{(1)})$, $(\bar{\mathbf{u}},\bar{\mathbf{v}})=(\mathbf{u}^{(1)},\ldots,\mathbf{u}^{(1)},\mathbf{v}^{(1)},\ldots,\mathbf{v}^{(1)})$ aus demselben eindim. Teilraum von $\mathbf{F}_{\mathbf{q}}^{2l}$, dann sind $(\mathbf{r}^{(i)},\mathbf{s}^{(i)})$ und $(\mathbf{u}^{(i)},\mathbf{v}^{(i)})$ jeweils aus demselben eindimensionalen Teilraum von $\mathbf{F}_{\mathbf{q}}^{2l}$ für alle $\mathbf{1} \leq i \leq l$. Also kommutieren nach Lemma 4.3 die $\mathbf{q} \times \mathbf{q}$ Matrizen $\mathbf{Z}(\mathbf{r}_{\alpha}^{(i)},\mathbf{s}_{\beta}^{(i)})$ und $\mathbf{Z}(\mathbf{u}_{\alpha}^{(i)},\mathbf{v}_{\beta}^{(i)})$ für alle $\mathbf{1} \leq i \leq l$ und damit auch ihre jeweiligen Tensorprodukte.

Sei nun L ein beliebiger der $[2^{l}]_{q} = (q^{2^{l}}-1)/(q-1)$ verschiedenen eindim. Teilräume von $F_{q}^{2^{l}}$. $\mathbf{Z}(L)$ sowie $\mathbf{\overline{Z}}(L)$ seien wie oben definiert.

4.8. LEMMA: In jedem $\overline{Z}(L)$ liegt eine selbstadj. $q^l \times q^l$ Matrix A_L mit q verschiedenen Eigenwerten und jeweiligen Eigenraumdimensionen q^{l-1} . Es gilt $\overline{Z}(L) = F(A_L)$. A_L ist bis auf die Wahl der Eigenwerte eindeutig bestimmt.

Bew.: Sei $(\bar{\mathbf{r}},\bar{\mathbf{s}})=(\mathbf{r}^{(i)},...,\mathbf{r}^{(i)},\mathbf{s}^{(i)},...,\mathbf{s}^{(i)})\in L$, und sei $(\bar{\mathbf{r}},\bar{\mathbf{s}})\neq (\bar{\emptyset},\bar{\emptyset})$. Dann ist $L(t):=(t\bar{\mathbf{r}},t\bar{\mathbf{s}})=(t\mathbf{r}^{(i)},...,t\mathbf{r}^{(i)},t\mathbf{s}^{(i)},...,t\mathbf{s}^{(i)})\in L$ für alle $t\in F_q$ und $L=\{L(t):\ t\in F_q\}$. Durch:

$$t \to \mathbf{Z}(\mathbf{L}(t))$$
 für alle $t \in \mathbf{F}_q$

ist eine Strahldarstellung von F_q als additive Gruppe gegeben. Die paarweise kommutierenden, normalen Matrizen $\mathbf{Z}(\mathbf{L}(\mathbf{t})) \in \mathbf{Z}(\mathbf{L})$ können gleichzeitig diagonalisiert werden. Die Strahldarstellung zerfällt

dann in lauter eindimensionale. Sei $t\to \varepsilon(t)$ mit $\varepsilon(t)\in\mathbb{C}$, $|\varepsilon(t)|=1$ für alle $t\in\mathbb{F}_a$, eine dieser Darstellungen. Dann ist

$$t \to \varepsilon^{-1}(t)\mathbf{Z}(\mathbf{L}(t))$$
 für alle $t \in \mathbf{F}_q$

eine gewöhnliche Darstellung von F_q als additive Gruppe. Die eindimensionalen solchen Darstellungen sind genau t $\rightarrow \chi(t)$, mit einem bel. additiven Charakter χ . Sei mit $F=F_q$:

$$P_{c}^{(L)} := \frac{1}{q} \sum_{t \in F} \overline{\chi}_{c}(t) \varepsilon^{-1}(t) Z(L(t)) \in \overline{Z}(L)$$

Mit (4.15) ist $P_c^{(L)}$ die orthog. Projektionsmatrix auf den Teilraum wo x_c auftritt. Dessen Dimension ist mit $\varepsilon(0) = \chi(0) = 1$ und (4.9):

$$\operatorname{tr}\left(P_{c}^{(L)}\right) = \operatorname{tr}\left(Z(\emptyset,\emptyset)\right)/q = q^{L-1}$$

Die 9 Projektionsmatrizen $P_c^{(L)}$, $c \in F_q$ bilden eine Zerlegung der Einheitsmatrix und spannen den 9-dim. Raum $\overline{Z}(L)$ auf. Sei nun:

$$\mathbf{A}_{\mathbf{L}} := \sum_{\mathbf{c} \in \mathbf{F}} \mathbf{a}_{\mathbf{c}} \mathbf{P}_{\mathbf{c}}^{(\mathbf{L})} \quad \text{mit } \mathbf{a}_{\mathbf{c}} \!\!=\!\! \mathbb{R} \text{ für alle } \mathbf{c} \!\!\in\!\! \mathbf{F}_{\mathbf{q}} \text{ und } \mathbf{a}_{\mathbf{c}} \!\!\neq\!\! \mathbf{a}_{\mathbf{c}}, \text{ für } \mathbf{c} \!\!\neq\!\! \mathbf{c}'$$

 $\mathbf{A_L} \in \overline{\mathbf{Z}}(\mathbf{L})$ und $\overline{\mathbf{Z}}(\mathbf{L}) = \mathbf{F}(\mathbf{A_L}) = \mathsf{Menge}$ der komplexen Linearkombinationen der $\mathbf{P_c^{(L)}}$, $\mathbf{c} \in \mathbf{F_q}$.

4.9. SATZ: $q=p^m$ sei eine Primzahlpotenz und $n=q^l$. Die n×n Matrizen $A_L \in \overline{\mathbb{Z}}(L)$ bilden eine vollständige Menge von $[2^l]_q = (q^{2^l}-1)/(q-1)$ selbstadj., paarweise bzgl. $\frac{1}{n}$ 1 unabhängigen Matrizen, mit jeweils q verschiedenen Eigenwerten und jeweiligen Eigenraumdimensionen q^{l-1} .

Bew.: Völlig analog zum Beweis von Satz 4.5. Die Vollständigkeit der Lösung zeigt Glong. (3.2).

4.10. BEISPIEL: Sehr einfach ist das für q=2 und bel. leN: Die eindim. Teilräume von $\mathbf{F}_{\mathbf{z}}^{21}$ enthalten jeweils 2 Punkte, den Nullpunkt und einen weiteren. Damit bestehen die $\mathbf{Z}(\mathbf{L})$ jeweils aus der Einheitsmatrix und einer der $2^{21}-1$ verschiedenen $2^{1}\times 2^{1}$ Matrizen $\mathbf{Z}(\bar{\mathbf{r}},\bar{\mathbf{s}})$. $\sigma_{\mathbf{x}}=\mathbf{W}(1,0)$, $\sigma_{\mathbf{y}}=i\mathbf{W}(1,1)$ und $\sigma_{\mathbf{z}}=\mathbf{W}(0,1)$ (siehe Beispiel 4.1) sind selbstadj., also auch bel. 1-fache Tensorprodukte der Einheitsmatrix 1 und von $\sigma_{\mathbf{x}}$, $\sigma_{\mathbf{y}}$, $\sigma_{\mathbf{z}}$ in bel. Anordnung. Diese Matrizen stimmen bis auf einen Faktor ± 1 oder $\pm i$ mit den $\mathbf{Z}(\bar{\mathbf{r}},\bar{\mathbf{s}})$ überein, liegen also jeweils in einem $\overline{\mathbf{Z}}(\mathbf{L})$. Die $2^{21}-1$ verschiedenen selbstadj. Ma-

trizen außer der Einheitsmatrix mit jeweils den zwei Eigenwerten ∓1 bilden also bereits eine vollständige Lösung, paarweise bzgl. ⁴¹ un-abhängiger selbstadj. 2¹×2¹ Matrizen. ■

4.11. Proposition: Die [21] Matrizen $A_{\rm L}$ von Lemma 4.8 und Satz 4.9 können in q¹+1 disjunkte Mengen zerlegt werden, mit jeweils [1] paarweise kommutierenden Matrizen in jeder Menge.

Bew.: Seien $(\gamma_1,\ldots,\gamma_l)$ und (η_1,\ldots,η_l) duale Basen des Körpers $\mathbf{F}_{\mathbf{q}}$, der Ordnung q'=q^l über dem Subkörper $\mathbf{F}_{\mathbf{q}}$. Seien \mathbf{r} , $\mathbf{s} \in \mathbf{F}_{\mathbf{q}}$.

$$\mathbf{r} = \mathbf{r}^{(i)} \gamma_{i} + \ldots + \mathbf{r}^{(i)} \gamma_{i} \text{ und } \mathbf{s} = \mathbf{s}^{(i)} \eta_{i} + \ldots + \mathbf{s}^{(i)} \eta_{i} \text{ mit } \mathbf{r}^{(i)}, \mathbf{s}^{(i)} \in \mathbb{F}_{q} \text{ für } \mathbf{1} \leq i \leq i$$

Das erlaubt eine Identifikation von $\mathbf{F}_{\mathbf{q}}^{\mathbf{2}}$, und $\mathbf{F}_{\mathbf{q}}^{\mathbf{2}\mathbf{1}}$ durch:

$$(\mathbf{r},\mathbf{s}) \in \mathbb{F}_q^2$$
, \leftrightarrow $(\mathbf{r}_{\gamma},\mathbf{s}_{\eta}) = (\mathbf{r}^{(1)},\ldots,\mathbf{r}^{(l)},\mathbf{s}^{(1)},\ldots,\mathbf{s}^{(l)}) \in \mathbb{F}_q^{2l}$

Die Zuordnung (Glchg.(4.17)) von \mathbf{F}_{q}^{2l} zu den $\mathbf{q}^{l} \times \mathbf{q}^{l}$ Matrizen $\mathbf{Z}(\overline{\mathbf{r}}, \overline{\mathbf{s}})$:

$$(\mathbf{r}^{(\mathbf{i})},...,\mathbf{r}^{(\mathbf{l})},\mathbf{s}^{(\mathbf{i})},...,\mathbf{s}^{(\mathbf{l})}) \; \leftrightarrow \; \mathbf{Z}(\mathbf{r}^{(\mathbf{i})}_{\alpha},\mathbf{s}^{(\mathbf{i})}_{\beta}) \otimes \ldots \otimes \mathbf{Z}(\mathbf{r}^{(\mathbf{l})}_{\alpha},\mathbf{s}^{(\mathbf{l})}_{\beta})$$

ist identisch mit der Zuordnung nach Glohg. (4.16) von F_{q}^{2} :

$$(\mathbf{r},\mathbf{s}) \leftrightarrow \mathbf{Z}(\mathbf{r}_{\xi},\mathbf{s}_{\vartheta})$$

mit den Basen von $\mathbf{F_q}$, über $\mathbf{F_p}$: $\xi = (\gamma_1 \alpha_1, \dots, \gamma_1 \alpha_m, \dots, \gamma_1 \alpha_1, \dots, \gamma_1 \alpha_m)$ und $\vartheta = (\eta_1 \beta_1, \dots, \eta_1 \beta_m, \dots, \eta_1 \beta_1, \dots, \eta_1 \beta_m)$. Aufgrund der Transitivität der Spur (4.11) folgt für alle $\mathbf{1} \leq \mathbf{i}, \mathbf{u} \leq \mathbf{i}, \mathbf{1} \leq \mathbf{j}, \mathbf{v} \leq \mathbf{m}$:

$$Tr(\gamma_i \alpha_j \eta_u \beta_v) = \begin{cases} 1 & \text{für } i=u \text{ und } j=v \\ \emptyset & \text{sonst} \end{cases}$$

d.h. die Dualität dieser beiden Basen. Also gilt Lemma 4.3 und die den eindim. Teilräumen M von F_q^2 , zugeordneten Matrizen in $\mathbf{Z}(\mathbf{M})$ und folglich alle Matrizen in $\mathbf{\overline{Z}}(\mathbf{M})$ kommutieren paarweise. Diese q'+1= q^L+1 verschiedenen Teilräume M von F_q^2 , sind als Teilräume von F_q^{2L} interpretiert jeweils L-dimensional. In jedem M liegen also $\begin{bmatrix} \mathbf{L} \end{bmatrix}_q$ verschiedene eindimensionalen Teilräume L von F_q^{2L} . Die zugeordneten $\mathbf{A}_L \in \mathbf{\overline{Z}}(\mathbf{M})$ kommutieren folglich.

Insbesondere folgt die Existenz von $[^1]_q$ paarweise kommutierenden und bzgl. $\frac{1}{n}$ 1 unabhängigen $q^l \times q^l$ Matrizen mit q verschiedenen Eigenwerten und jeweiligen Eigenraumdimensionen q^{l-1} . Das sind vollständige klassische Lösungen, die orthogonalen Anordnungen entsprechen:

4.12. KOROLLAR: Es gibt vollständige orthogonale Anordnungen des Typs: $OA(q^l,[\iota]_q,q,2)$ mit dem Index q^{l-z} . Für $\iota=2$ entspricht das q-1 paarweise orthogonalen Lateinischen Quadraten.

Diese Resultat ist wohlbekannt und die in der Literatur angegebenen Konstruktionen sind äquivalent zu unserer. (Siehe Raghavarao [36], \$2.3, oder Beth/Jungnickel/Lenz [07] Prop. I.7.10 in der Sprache Transversaler Designs, oder Dénes/Keedwell [20], \$5.2 für Lateinische Quadrate.)

Satz 4.9 liefert klassische und neue Resultate aus einem Prinzip. Setzen wir die klass. Lösungen als bekannt voraus so folgt die Existenz der Lösungen von Satz 4.9 aber auch sofort mit folgendem einfachen Lemma aus Satz 4.5:

4.13. LEMMA: Angenommen es gibt r bzgl. der Gleichverteilung unabhängige Zufallsvariablen \mathbf{f}_i , $\mathbf{1} \le i \le r$ über einer n-elementigen Menge Ω und es gibt s bzgl. $\frac{\mathbf{1}}{n}$ 1 unabhängige, selbstadj. und nichtentartete n×n Matrizen \mathbf{A}_j , $\mathbf{1} \le j \le s$. Dann gibt es r.s bzgl. $\frac{\mathbf{1}}{n}$ 1 unabhängige, selbstadj. n×n Matrizen $\mathbf{B}_{i,j}$, $\mathbf{1} \le i \le r$, $\mathbf{1} \le j \le s$. Für alle $\mathbf{1} \le i \le r$ haben $\mathbf{B}_{i,1}$, ..., $\mathbf{B}_{i,s}$ jeweils dieselbe Anzahl verschiedener Eigenwerte mit derselben Vielfachheit, wie \mathbf{f}_i Werte hat.

Bew.: O.B.d.A. kann $\Omega=\{1,\ldots,n\}$ gesetzt werden und die n verschiedenen Eigenwerte von A_j jeweils als: 1,...,n angenommen werden für alle $1 \le j \le n$. Dann ist

$$B_{ij} := f_i(A_j)$$
 für $i \le i \le r$, $i \le j \le s$

- über die Diagonalform der A_j - wohldefiniert.

f_i(A_j) und f_k(A_l), i≤i,k≤r, i≤j,l≤s sind für j≠l als Funktionen von bzgl.

f¹ unabhängigen Matrizen A_j und A_l unabhängig bzgl. f¹ . (siehe Prop. 2.4). Für j=l,i≠k folgt ihre Unabhängigkeit bzgl. f¹ als kommutierende Matrizen aus jener der klass. Zufallsvariablen f; und f_k.

Nach Prop.4.11 entsprechen die Lösungen von Satz 4.9 denen die man aus $OA(q^1,[1]_q,q,2)$ und den Lösungen von Satz 4.5 wie eben beschrieben erhält.

4.3. ZUGEORDNETE VH- BZW. VBH-MATRIZEN

Den Lösungen von Satz 4.5 sind 9 VH-Matrizen der Ordnung 9 mit Produkteigenschaft zugeordnet.

Für q=2 sind zwei 2×2 VH-Matrizen $\mathbf{v_o}$ und $\mathbf{v_i}$ in Beispiel 4.1 angeführt, für q=4 siehe die vier 4×4 VH-Matrizen $\mathbf{v_a}$, $\mathbf{a} \in \mathbf{F_i}$ in Beispiel 4.6. Für alle ungeraden q können sogar leicht explizite Formeln für q zugeordnete VH-Matrizen angegeben werden.

Seien für eine bel. Primzahl p die Standardbasisvektoren von $\mathbb{C}^{\mathtt{P}}$:

$$e_0 = (1,0,\ldots,0)^T$$
, $e_i = (0,1,0,\ldots,0)^T$, ..., $e_{p-i} = (0,\ldots,0,1)^T$

Die Indizes \circ , ι , ..., p-1 seien mit den Elementen von \mathbb{Z}_p identifiziert. Mit $\lambda=e^{i2\pi/p}$ gilt für alle r, s, $x\in\mathbb{Z}_p$ für die $p\times p$ Weylmatrizen:

$$W(r,s)e_x = \lambda^{sx}e_{x-r}$$

Seien $\mathbf{x}=(\mathbf{x_1},\ldots,\mathbf{x_m})$ ein bel. m-tupel von Elementen $\mathbf{x_i}\in\mathbb{Z}_p$, $\mathbf{1}\leq\mathbf{i}\leq\mathbf{m}$. Sei:

$$e_x := e_{\chi_4} \otimes \ldots \otimes e_{\chi_m}$$
 (4.18)

Die q=p[™] verschiedenen e, bilden eine Basis des C^q. Mit (4.6) folgt:

$$Z(r,s)e_{v} = \lambda^{\langle s|x\rangle}e_{v-r}$$
 (4.19)

Sei nun mit zwei dualen Basen $\alpha = (\alpha_1, \ldots, \alpha_m)$ und $\beta = (\beta_1, \ldots, \beta_m)$ von \mathbf{F}_q über \mathbf{F}_p entsprechend (4.16): $\mathbf{r}, \mathbf{s} \in \mathbf{F}_q \leftrightarrow \mathbf{Z}(\mathbf{r}_\alpha, \mathbf{s}_\beta)$. Ebenso ist durch $\mathbf{x} \leftrightarrow \mathbf{x}_\alpha \leftrightarrow \mathbf{e}_{\mathbf{x}}$ eine ein-eindeutige Zuordnung von $\mathbf{x} \in \mathbf{F}_q$ zu den q verschiedenen Basisvektoren (4.18) gegeben.

Aus (4.13) folgt: $\langle s_{\beta} | x_{\alpha} \rangle = Tr(sx)$ und damit wird (4.19) zu:

$$Z(r_{\alpha}, s_{\beta}) e_{x_{\alpha}} = \lambda^{Tr(sx)} e_{x_{\alpha}-r_{\alpha}} = \chi_{i}(sx) e_{(x-r)_{\alpha}}$$

mit dem kanonischen Charakter x_i von F_a (siehe Glchg.(4.14).

Wir definieren weiters für bel. $\mathbf{a} \in \mathbf{F}_q = \mathbf{F}$ durch :

$$U_a e_{x_\alpha} = \sqrt{\frac{1}{q}} \sum_{y \in F} \chi_i (ay^2 + xy) e_{y_\alpha}$$

q×q Matrizen υ,

4.14. LEMMA: U_a ist eine unitäre q×q Matrix für alle $a \in F_q$.

Bew.: $\mathbf{U}_{\mathbf{a}}^* = \mathbf{U}_{\mathbf{a}}^{-1}$ da für beliebige Basisvektoren $\mathbf{e}_{\mathbf{x}_{\mathbf{a}}}$, $\mathbf{x} \in \mathbf{F}_{\mathbf{q}} = \mathbf{F}$ gilt:

$$\begin{aligned} \mathbf{U}_{\mathbf{a}}^{*}\mathbf{U}_{\mathbf{a}}\mathbf{e}_{\mathbf{x}_{\alpha}} &= \frac{\mathbf{i}}{q} \sum_{\mathbf{z} \in \mathbf{F}} \sum_{\mathbf{y} \in \mathbf{F}} \bar{\chi}_{\mathbf{i}} (\mathbf{a}\mathbf{y}^{2} + \mathbf{z}\mathbf{y}) \chi_{\mathbf{i}} (\mathbf{a}\mathbf{y}^{2} + \mathbf{x}\mathbf{y}) \mathbf{e}_{\mathbf{Z}_{\alpha}} \\ &= \frac{\mathbf{i}}{q} \sum_{\mathbf{z} \in \mathbf{F}} \left(\sum_{\mathbf{y} \in \mathbf{F}} \chi_{\mathbf{i}} (\mathbf{y} (\mathbf{x} - \mathbf{z})) \right) \mathbf{e}_{\mathbf{Z}_{\alpha}} \\ &= \mathbf{e}_{\mathbf{x}_{\alpha}}. \quad (\text{siehe} (4.15)) \end{aligned}$$

Das folgt auch sofort, wenn man bemerkt, daß:

$$U_a = D_a TP$$

wobei:i) $\mathbf{D_a} \mathbf{e_x} = \chi_{\mathbf{i}}(\mathbf{x}^2) \mathbf{e_x}$ eine (unitäre) Diagonalmatrix ist.

ii) $\mathbf{Te}_{\mathbf{x}} = \sqrt{\frac{1}{q}} \sum_{\mathbf{y} \in \mathbf{Z}} \lambda^{\langle \mathbf{x} \mid \mathbf{y} \rangle} \mathbf{e}_{\mathbf{y}}$, $(\mathbf{Z} = \mathbb{Z}_p^m)$, Durch Vergleich ist leicht zu

sehen, daß $T = F_{(p)} \otimes ... \otimes F_{(p)}$, d.h. das m-fache Tensorprodukt der in der Einleitung definierten p×p Fouriermatrix $F_{(p)}$ ist.

iii) $Pe_{\mathbf{x}} = e_{\mathbf{x}}$, ist eine Permutationsmatrix, wobei falls $\mathbf{x} = \mathbf{x}_{\alpha} \Rightarrow \mathbf{x}' = \mathbf{x}_{\beta}$.

Insbesondere ist damit $\mathbf{U}_{\mathbf{a}}$ für alle $\mathbf{a} \in \mathbf{F}$ im Sinne von Def.3.2 äquivalent zum m-fachen Tensorprodukt der pxp Fouriermatrix $\mathbf{F}_{(p)}$.

4.15. LEMMA: Für alle a,r,s∈F =F gilt:

$$\mathbf{U}_{\mathbf{a}}^{-1}\mathbf{Z}(\mathbf{r}_{\alpha},\mathbf{s}_{\beta})\mathbf{U}_{\mathbf{a}} = \chi_{\mathbf{i}}(\mathbf{ar}^2 + \mathbf{sr})\mathbf{Z}(-(2\mathbf{ar} + \mathbf{s})_{\alpha},\mathbf{r}_{\beta})$$

Bew.: Für beliebige Basisvektoren e_{x₂}, ×∈F_q=F gilt:

$$\begin{split} Z(r_{\alpha},s_{\beta}) \mathbf{U}_{\mathbf{a}} \mathbf{e}_{\mathbf{x}_{\alpha}} &= Z(r_{\alpha},s_{\beta}) \sqrt{q} \sum_{\mathbf{y} \in F} \chi_{\mathbf{i}} (\mathbf{a}\mathbf{y}^{2} + \mathbf{x}\mathbf{y}) \mathbf{e}_{\mathbf{y}_{\alpha}} \\ &= \sqrt{q} \sum_{\mathbf{y} \in F} \chi_{\mathbf{i}} (\mathbf{a}\mathbf{y}^{2} + \mathbf{x}\mathbf{y} + \mathbf{s}\mathbf{y}) \mathbf{e}_{(\mathbf{y} - \mathbf{r})_{\alpha}} \quad (\text{Sei } \mathbf{z} := \mathbf{y} - \mathbf{r}) \\ &= \chi_{\mathbf{i}} (\mathbf{a}\mathbf{r}^{2} + \mathbf{x}\mathbf{r} + \mathbf{s}\mathbf{r}) \sqrt{q} \sum_{\mathbf{z} \in F} \chi_{\mathbf{i}} (\mathbf{a}\mathbf{z}^{2} + (2\mathbf{a}\mathbf{r} + \mathbf{x} + \mathbf{s})\mathbf{z}) \mathbf{e}_{\mathbf{z}_{\alpha}} \\ &= \chi_{\mathbf{i}} (\mathbf{a}\mathbf{r}^{2} + \mathbf{s}\mathbf{r}) \chi_{\mathbf{i}} (\mathbf{x}\mathbf{r}) \mathbf{U}_{\mathbf{a}} \mathbf{e}_{(2\mathbf{a}\mathbf{r} + \mathbf{x} + \mathbf{s})_{\alpha}} \\ &= \mathbf{U}_{\mathbf{a}} \chi_{\mathbf{i}} (\mathbf{a}\mathbf{r}^{2} + \mathbf{s}\mathbf{r}) Z(-(2\mathbf{a}\mathbf{r} + \mathbf{s})_{\alpha}, r_{\beta}) \mathbf{e}_{\mathbf{x}_{\alpha}} \end{split}$$

4.16. SATZ: Sei $q=p^m$ eine ungerade Primzahlpotenz (p>2). Dann sind die q Matrizen $\mathbf{U_a}$, $\mathbf{a} \in \mathbf{F_q}$ eine den Lösungen von Satz 4.5 zugeordnete vollständige Menge von VH-Matrizen mit Produkteigenschaft.

Bew.: $\mathbf{U_a}$ sind VH-Matrizen, da sie unitär sind und die Einträge alle Absolutbetrag $\sqrt{\frac{1}{q}}$ haben. Die eindimensionalen Teilräume von $\mathbf{F_q^2}$ sind:

$$S=\left\{ \begin{array}{ll} (\emptyset,s) & :s\in F_q \end{array} \right\} \quad \text{und} \quad T_c=\left\{ \begin{array}{ll} (r,rc): \; r\in F_q \end{array} \right\} \quad \text{für c} \in F_q$$

Alle Matrizen in $\mathbf{Z}(S)$ sind diagonal, also auch $\mathbf{A}_S \in \overline{\mathbf{Z}}(S)$. Sei nun: $\mathbf{a} = -\mathbf{c}/\mathbf{Z} \in \mathbf{F}_q$ (2≠0! in \mathbf{F}_q für ungerade q). Dann folgt mit Lemma 4.15:

$$U_{\mathbf{a}}^{-1}\mathbf{Z}(\mathbf{r}_{\alpha}, (\mathbf{rc})_{\beta})U_{\mathbf{a}} = \chi_{\mathbf{i}}(\mathbf{cr}^{2}/2)\mathbf{Z}(\emptyset, \mathbf{r}_{\beta}) \in \overline{\mathbf{Z}}(\mathbf{S})$$

d.h. für bel. Teilräume $L=T_c$ werden alle Matrizen in $\mathbf{Z}(L)$ und damit auch $\mathbf{A_L} \in \overline{\mathbf{Z}}(L)$ durch die VH-Matrix $\mathbf{U_{-c/2}}$ diagonalisiert. Mit $\mathbf{c} \in \mathbf{F_q}$ durchläuft auch $-\mathbf{c}/\mathbf{Z}$ ganz $\mathbf{F_q}$.

Wird die Zuordnung zu Satz 4.5 nicht weiter berücksichtigt, dann gilt allgemeiner:

4.17. Korollar: Seien $k_1, \ldots k_q$ die Elemente von F_q mit ungeradem q in beliebiger Reihenfolge und χ ein nichttrivialer, additiver Charakter. Die

$$\mathbf{X}_{\mathbf{a}} = \sqrt{\frac{1}{q}} \begin{bmatrix} \chi(\mathbf{ak_{1}^{2}} + \mathbf{k_{1}^{2}}) & \chi(\mathbf{ak_{1}^{2}} + \mathbf{k_{1}^{2}} \mathbf{k_{2}}) & \dots & \chi(\mathbf{ak_{1}^{2}} + \mathbf{k_{1}^{2}} \mathbf{k_{q}}) \\ \chi(\mathbf{ak_{2}^{2}} + \mathbf{k_{2}^{2}} \mathbf{k_{1}}) & \chi(\mathbf{ak_{2}^{2}} + \mathbf{k_{2}^{2}}) & \dots & \chi(\mathbf{ak_{2}^{2}} + \mathbf{k_{2}^{2}} \mathbf{k_{q}}) \\ \vdots & \vdots & & \vdots & & \vdots \\ \chi(\mathbf{ak_{q}^{2}} + \mathbf{k_{q}^{2}} \mathbf{k_{1}}) & \chi(\mathbf{ak_{q}^{2}} + \mathbf{k_{q}^{2}} \mathbf{k_{2}}) & \dots & \chi(\mathbf{ak_{q}^{2}} + \mathbf{k_{q}^{2}}) \end{bmatrix} \quad \mathbf{a} \in \mathbf{F}_{q}$$

bilden eine (vollständige) Menge von q VH-Matrizen der Ordnung q mit Produkteigenschaft.

 $\mathbf{X_a} + \mathbf{X_{ca}} \mathbf{Q} = \mathbf{P^{-i}} \mathbf{U_{ca}} \mathbf{PQ}$, mit einer weiteren Permutationsmatrix \mathbf{Q} . Die Lösungen von Satz 4.16 und Korollar 4.17 sind also im Sinne der Definition 3.2' alle äquivalent.

Die Produkteigenschaft der $\mathbf{X_a}$, $\mathbf{a} \in \mathbf{F_q}$ läßt sich auch explizit überprüfen. Aus Theorem 5.15 über Gaußsummen und Theorem 5.33 in Lidl/ Niederreiter [31] folgt, daß für nichttriviale, additive Charaktere \mathbf{x} von $\mathbf{F} = \mathbf{F_q}$ mit ungeradem q, für alle $\mathbf{c} \neq \emptyset$, $\mathbf{d} \in \mathbf{F}$ gilt:

$$\sum_{\mathbf{x} \in \mathbf{F}} \chi(\mathbf{cx}^2 + \mathbf{dx}) = \sqrt{\mathbf{q}}$$

Das ist, wie man sofort sieht, äquivalent dazu, daß die Einträge von $\mathbf{X}_{\mathbf{a}}^{-1}\mathbf{X}_{\mathbf{b}}$ für $\mathbf{a} \neq \mathbf{b}$ alle den Absolutbetrag $\sqrt{\frac{1}{2}}$ haben.

4.18. BEISPIEL: Drei entsprechend konstruierte 3×3 VH-Matrizen mit Produkteigenschaft sind mit $\lambda=e^{i2\pi/3}$:

$$\mathbf{U_{O}} = \sqrt{\frac{1}{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \lambda & \lambda^{2} \\ 1 & \lambda^{2} & \lambda \end{bmatrix} \qquad \mathbf{U_{i}} = \sqrt{\frac{1}{3}} \begin{bmatrix} 1 & 1 & 1 \\ \lambda & \lambda^{2} & 1 \\ \lambda & 1 & \lambda^{2} \end{bmatrix} \qquad \mathbf{U_{2}} = \sqrt{\frac{1}{3}} \begin{bmatrix} 1 & 1 & 1 \\ \lambda^{2} & 1 & \lambda \\ \lambda^{2} & \lambda & 1 \end{bmatrix}$$

Ein offenes Problem ist es noch explizite Formeln für 9 VH-Matrizen mit Produkteigenschaft der Ordnung $9=2^m$, melN zu bestimmen.

Noch kurz einige Bemerkungen zu den $[2l]_q^{-1}$ VBH-Matrizen der Ordnung q^l mit Subblöcken der Ordnung q^{l-1} , die den Lösungen von Satz 4.9 zugeordnet sind:

Entsprechend der Konstruktion im Beweis von Proposition 4.11 können $\mathbf{q'} = \mathbf{q^l}$ VH-Matrizen: $\mathbf{U_1}, \dots, \mathbf{U_q}$, der Ordnung $\mathbf{q^l}$ zugeordnet werden, die jeweils $[\mathbf{l}]_{\mathbf{q}}$ kommutierende $\mathbf{A_L}$ gleichzeitig diagonalisieren, nicht notwendig aber in geordnete Gestalt. Zu den $[\mathbf{l}]_{\mathbf{q}}$ kommutierenden $\mathbf{A_L}$ für sich wiederum gehören $\mathbf{k} = [\mathbf{l}]_{\mathbf{q}} - 1$ Permutationsmatrizen als VBH-Matrizen: $\mathbf{P_1}, \dots, \mathbf{P_k}$. Die Menge:

{
$$XY : X \in \{1, U_1, ..., U_q, \}, Y \in \{1, P_1, ..., P_k\}, XY \neq 1}$$

enthält $(q'+1)(k+1)-1 = ((q^l+1)(q^l-1)/(q-1))-1 = [2l]_q-1 \ VBH-Matrizen.$ Sie bilden das gesuchte vollständige Lösungssystem.

4.4. LOSUNGEN FUR n≠p™

n×n Weylmatrizen W(r,s), r,s∈Z_n bzw. deren Tensorprodukte, lassen sich auch für Nichtprimzahlpotenzen n benützen um Mengen von paarweise bzgl. ½1 unabhängiger, selbstadj. Matrizen zu konstruieren. Diese sind aber nicht vollständig. Wir skizzieren einige Ideen:

Sei z.B. für ein bel. n∈N:

 $\begin{array}{c} R=\{(s,s)\colon s\in\mathbb{Z}_n\},\ S=\{(0,s)\colon s\in\mathbb{Z}_n\},\ T=\{(s,0)\colon s\in\mathbb{Z}_n\}\\ \text{Das sind drei bis auf den Nullpunkt }(0,0)\ \text{disjunkte Teilmengen von }\mathbb{Z}_n\times\mathbb{Z}_n\ \text{mit jeweils n Elementen. Sei }\mathbf{W}(\mathbf{L})\ \text{für }\mathbf{L}=R,S\ \text{oder T die Menge der n Weylmatrizen }\mathbf{W}(r,s),\ (r,s)\in\mathbf{L}\ \text{und }\overline{\mathbf{W}}(\mathbf{L})\ \text{die Menge der komplexen }\mathbf{L}\ \text{inearkombinationen der Matrizen in }\mathbf{W}(\mathbf{L}). \end{aligned}$

4.19. Lemma: In jedem $\overline{\mathbf{W}}(\mathbf{L})$, $\mathbf{L}=\mathbf{R},\mathbf{S}$ oder T liegt eine nichtentartete, selbstadj. Matrix $\mathbf{A}_{\mathbf{L}}\in\overline{\mathbf{W}}(\mathbf{L})$. Die drei Matrizen $\mathbf{A}_{\mathbf{R}},\mathbf{A}_{\mathbf{S}},\mathbf{A}_{\mathbf{T}}$ sind paarweise bzgl. 1 unabhängig.

Bew.: Sei L=R,S oder T. Nach (4.5) kommutieren alle Matrizen in $\mathbf{W}(\mathbf{L})$ paarweise. Analog zu Lemma 4.4 schließen wir, daß es eine nichtentartete, selbstadj. Matrix $\mathbf{A_L}$ als eine Linearkombination der n kommutierenden und paarweise orthogonalen (siehe Glchg. (4.4)) Matrizen aus $\mathbf{W}(\mathbf{L})$ gibt und damit $\mathbf{F}(\mathbf{A_L}) = \overline{\mathbf{W}}(\mathbf{L})$ gilt. Wieder völlig analog wie im Beweis von Satz 4.5 folgt das Ergebnis.

Wir erhalten das in Kap.3 Absch.1 angekündigte Resultat $A_{n,3} \ge 1$. Im allgemeinen (z.B. für n=6) gibt es keine weitere n-elementige Teilmenge M von $\mathbb{Z}_n \times \mathbb{Z}_n$, die bis auf den Nullpunkt disjunkt zu R,S und T ist und wo alle Matrizen in $\mathbf{W}(\mathbf{M})$ kommutieren. Falls doch weitere solche Mengen existieren, können mit $\mathbf{A}_{\mathbf{M}} \in \overline{\mathbf{W}}(\mathbf{M})$ auch weitere paarweise bzgl. $\frac{1}{n}$ 1 unabhängige, selbstadj. Matrizen gebildet werden.

4.20. LEMMA: A_R , A_S und A_T sind folgende zwei VH-Matrizen mit Produkt-eigenschaft zugeordnet: U_1 =F $_{(n)}$ und U_2 =DF $_{(n)}$, wobei F $_{(n)}$ die n×n Four-iermatrix ist und: D=diag $(1, \varepsilon^{-1}, \varepsilon^{-4}, \varepsilon^{-9}, \dots, \varepsilon^{-(n-1)^2})$, mit ε = $-e^{i\pi/n}$.

Bew.: $\mathbf{W}(0,s) = \mathbf{U}^s$ sind für alle $s \in \mathbb{Z}_n$ diagonal, also auch \mathbf{A}_s . Es ist leicht zu sehen, daß: $\mathbf{F}^{-1}\mathbf{W}(r,s)\mathbf{F}^{-1}\mathbf{W}(r,s)$ = $\mathbf{W}(-s,r)$ mit der n×n Fouriermatrix $\mathbf{F}^{-1}\mathbf{W}(r,s)$. Speziell: $\mathbf{F}^{-1}\mathbf{W}(r,0)\mathbf{F}^{-1}\mathbf{W}(r,s)$ = \mathbf{U}^r , d.h. $\mathbf{F}^{-1}\mathbf{W}(r,s)$ diagonalisiert alle $\mathbf{W}(r,s)$, also auch \mathbf{A}_s . Weiters gilt:

$$D^{-1}VD = \varepsilon VU^{-1} \quad \text{und} \quad D^{-1}UD = U$$

$$D^{-1}W(r,s)D = \varepsilon^{r}W(r,-r+s)$$

$$(DF(rx))^{-1}W(s,s)(DF(rx)) = \varepsilon^{s}U^{s}$$

d.h. DF(m) diagonalisiert W(s,s) für alle $s \in \mathbb{Z}_n$, also auch A_R .

Es liegt weiters nahe mehrfache Tensorprodukte von Weylmatrizen verschiedener Ordnung zu betrachten (es genügt Primzahlpotenzordnungen zu nehmen). Die so entstehenden n×n Matrizen sind paarweise orthogonal auf M_n. Analog wie oben kann nun versucht werden diese n² verschiedenen Matrizen in Teilmengen kommutierender Matrizen zu zerlegen und so zu paarweise bzgl.½1 unabhängigen, selbstadj. n×n Matrizen zu gelangen. Eine systematische Untersuchung hiervon bleibt noch vorbehalten.

Es ist leicht zu sehen, daß die Anwendung von Korollar 3.8 auf die konstruierten, vollständigen Lösungen, d.h. einfach Bildung ihrer Tensorprodukte, ein Spezialfall dieses Ansatzes ist:

4.21. Korollar: Sei $n=q_1^{l_1}\dots q_m^{l_m}$, mit paarweise teilerfremden Primzahlpotenzen q_i und l_i \in N, für alle $1 \le i \le m$. Dann gibt es

$$k = \min \left[[21_{i}]_{q_{i}}, \dots, [21_{m}]_{q_{m}} \right]$$

paarweise bzgl. $\frac{1}{n}$ 1 unabhängige, selbstadj. n×n Matrizen, mit jeweils $q=q_1\dots q_m$ verschiedenen Eigenwerten. Für $n=q_1\dots q_m$ gibt es insbesondere k=min $(q_1,\dots,q_m)+1$ paarweise bzgl. $\frac{1}{n}$ 1 unabhängige, nichtentartete, selbstadj. n×n Matrizen. $(k\geq 3$ für alle $n\in \mathbb{N}$).

Eingeschränkt auf die klassischen Lösungen (kommutierende Matrizen) entspricht Korollar 4.21 dem Satz von Mac Neish für Orthogonale Anordnungen. (Siehe Beth/Jungnickel/Lenz [07], Satz I.7.7, in der Terminologie Transversaler Designs)

5. VBH-MATRIZEN, VH-MATRIZEN UND DEREN PRODUKTE

Der erste Abschnitt enthält zwei einfache Beiträge zur allgemeinen Theorie der VBH-Matrizen. Im zweiten bzw. dritten Abschnitt werden spezielle Konstruktionen von n×n VH-Matrizen bzw. Paaren solcher Matrizen mit Produkteigenschaft angegeben, welche im besonderen in dem Bemühen resultieren entsprechende Lösungen für n=6 zu bestimmen. Aus Satz 4.5 folgt, daß für bel. Primzahlpotenzen q vollständige Mengen von q VH-Matrizen der Ordnung q mit Produkteigenschaft existieren. (Korollar 4.17 gibt explizite Formeln für ungerade q). Für die kleinste Nichtprimzahlpotenz 6 legen die hier gewonnenen Ergebnisse hingegen die Vermutung nahe, daß nicht einmal drei 6×6 VH-Matrizen mit Produkteigenschaft existieren.

5.1. VBH-MATRIZEN

Entsprechend der Bemerkung im Anschluß an Definition 1.1 ist der einfachste nichttriviale Fall zweier bzgl. $\frac{1}{n}$ 1 unabhängiger, selbstadjungierter n×n Matrizen jener, wenn beide Matrizen jeweils genau zwei verschiedene Eigenwerte haben. Seien diese (o.B.d.A.) als 0 und 1 angenommen. Dann sind beides Projektionsmatrizen: P,Q ($\not\approx$ 0,1). Ihre Unabhängigkeit bzgl. $\frac{1}{n}$ 1 entspricht: $\text{tr}(PQ) = \frac{1}{n} \text{tr}(P) \text{tr}(Q)$. Zugeordnet sind die einfachsten nichttrivialen VBH-Matrizen, jene mit vier Subblöcken (die sich nicht über ganze Zeilen oder Spalten erstrecken). Wir analysieren hier der Kürze halber nur den Fall quadratischer Subblöcke:

5.1. PROPOSITION: Jede 2m×2m VBH(m,m;m,m)-Matrix , m∈N, ist zu einer der folgenden solchen Matrizen äquivalent:

$$U = \left[\begin{array}{cc} X & Y \\ Y & -X \end{array} \right]$$

 $\mbox{mit mmm Submatrizen } \mathbf{X} = \mbox{diag}(\mathbf{x_i}, \dots, \mathbf{x_m}) \ \mbox{und } \mathbf{Y} = \mbox{diag}(\mathbf{y_i}, \dots, \mathbf{y_m}) \,, \ \mbox{wobei}$

i) $0 \le x_i$, $y_i \le 1$ und $x_i^2 + y_i^2 = 1$ für alle $i \le i \le m$ und

ii)
$$x_1^2 + x_2^2 + ... + x_m^2 = \frac{m}{2}$$
 gilt.

Beweis: Es ist leicht nachzuprüfen, daß jedes solche ${\bf v}$ eine ${\bf v}$ VBH(m,m;m,m)-Matrix ist. Sei nun

$$V = \begin{bmatrix} X & R \\ Y & S \end{bmatrix}$$

eine bel. 2m×2m VBH(m,m;m,m)-Matrix mit m×m Submatrizen X,Y,R und S. Der wesentliche Schritt ist, daß wir entsprechend den Bemerkungen im Anschluß an Def. 3.2 (auf Seite 34) annehmen können, daß V in sogen. Normalform vorliegt, d.h. X,Y und R bereits zu positiv semidefiniten Matrizen gemacht wurden. X kann dabei sogar als diagonalisiert angenommen werden. Sei also:

 $X=diag(x_1,...,x_m)$ mit $x_i \ge 0$ für alle $\le i \le m$.

Nach Vorraussetzung ist $x_i^2 + ... + x_m^2 = ||X||^2 = \frac{m}{2}$ erfüllt. Aus $VV^* = V^*V = 1$ folgt:

$$X^*X + Y^*Y = XX^* + RR^* = 1$$

 $\Rightarrow R^2 = Y^2 = 1 - X^2$

Die eindeutige positiv semidefinite Quadratwurzel aus 1-X² ist:

 $R=Y=\text{diag}(\textbf{y}_{i},\ldots,\textbf{y}_{m})\text{, mit }\textbf{y}_{i}\geq\emptyset\text{ und }\textbf{x}_{i}^{2}+\textbf{y}_{i}^{2}=1\text{ für alle }i\leq i\leq m\text{.}$

Aus $vv^* = v^*v = 1$ erhalten wir weiters:

$$Y(X+S) = (X+S)Y = \emptyset$$
 (5.1)

Falls \mathbf{Y} invertierbar ist, folgt sofort $\mathbf{S} = -\mathbf{X}$, womit alles gezeigt wäre.

Der Fall eines nichtinvertierbaren Y benötigt etwas zusätzliche Arbeit: Sei Y (durch gleichzeitige Permutation von X,Y und S) von folgender Form: Y=diag(y_1,\ldots,y_r ,0,...,0) mit y_1,\ldots,y_r >0 für ein 0≤r<m, Dann ist X=diag(x_1,\ldots,x_r ,1,...,1). Sei nun

$$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix}$$

so partitioniert, daß S_{11} eine r×r Matrix ist. Aus (5.1) folgt sofort, daß S_{11} =diag(-x₁,...,-x_r) und S_{21} = S_{12} =0 gilt. Mit der Unitarität von V folgt, daß S_{22} eine unitäre (m-r)×(m-r) Matrix ist. Sei

$$W = \begin{bmatrix} 1_r & \emptyset \\ \emptyset & -S_{22}^{-1} \end{bmatrix}$$

Wird die untere Blockzeile von V mit der unitären m×m Matrix W von links multipliziert, was einer Äquivalenzoperation entspricht, so bleibt Y unverändert und S wird zu -X.

Das Tensor- oder Kronecker-Produkt von VH-Matrizen ist eine ebensolche. Entsprechend findet es in der Theorie gewöhnlicher und verallgemeinerter Hadamard-Matrizen vielfache Anwendung. Wir geben eine Verallgemeinerung auf VBH-Matrizen an.

5.2. Proposition: Seien

$$U = \begin{bmatrix} U_{1i} & U_{12} & \dots & U_{1s} \\ U_{2i} & U_{22} & \dots & U_{2s} \\ \vdots & \vdots & & \vdots \\ U_{ri} & U_{r2} & \dots & U_{rs} \end{bmatrix} \qquad V = \begin{bmatrix} V_{1i} & V_{12} & \dots & V_{1q} \\ V_{2i} & V_{22} & \dots & V_{2q} \\ \vdots & \vdots & & \vdots \\ V_{pi} & V_{p2} & \dots & V_{pq} \end{bmatrix}$$

eine n×n bzw. eine m×m VBH-Matrix, mit zugehörigen Submatrizen: U_{ij}, 1≤i≤r, 1≤j≤s, bzw. V_{kl}, 1≤k≤p, 1≤l≤q. Dann ist

$$U \otimes_{\mathbf{B}} V := \begin{bmatrix} U_{11} \otimes_{11} & U_{12} \otimes_{12} & \dots & U_{13} \otimes_{14} & \dots & U_{18} \otimes_{14} & \dots & U_{18} \otimes_{14} \\ U_{11} \otimes_{21} & U_{12} \otimes_{22} & \dots & U_{14} \otimes_{2q} & \dots & U_{18} \otimes_{24} & \dots & U_{18} \otimes_{2q} \\ \vdots & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ U_{11} \otimes_{11} & \otimes_{11} \otimes_{12} & \dots & U_{11} \otimes_{1q} & \dots & U_{18} \otimes_{p_1} & \dots & U_{18} \otimes_{p_q} \\ \vdots & \vdots & & & & & & & & & & & & & & \\ U_{11} \otimes_{11} & \otimes_{11} \otimes_{12} & \dots & U_{18} \otimes_{p_q} & \dots & U_{18} \otimes_{p_1} & \dots & U_{18} \otimes_{p_q} \\ \vdots & \vdots & & & & & & & & & & & & & \\ U_{11} \otimes_{11} & \otimes_{11} \otimes_{12} & \dots & U_{18} \otimes_{1q} & \dots & U_{18} \otimes_{p_1} & \dots & U_{18} \otimes_{p_q} \\ \vdots & \vdots & & & & & & & & & & & & & \\ U_{11} \otimes_{11} & \otimes_{12} & \dots & U_{18} \otimes_{1q} & \dots & U_{18} \otimes_{p_1} & \dots & U_{18} \otimes_{p_q} \\ \vdots & \vdots & & & & & & & & & & & \\ U_{11} \otimes_{11} & \otimes_{12} & \dots & U_{18} \otimes_{1q} & \dots & U_{18} \otimes_{p_1} & \dots & U_{18} \otimes_{p_q} \\ \vdots & \vdots & & & & & & & & & & & \\ U_{11} \otimes_{11} & \otimes_{12} & \dots & U_{18} \otimes_{1q} & \dots & U_{18} \otimes_{p_1} & \dots & U_{18} \otimes_{p_q} \\ \vdots & \vdots & & & & & & & & & & & \\ U_{11} \otimes_{11} & \otimes_{11} \\ \vdots & \vdots & & & & & & & & & & & & \\ U_{11} \otimes_{11} & \otimes_{11} \\ \vdots & \vdots & & & & & & & & & & & \\ U_{11} \otimes_{11} & \otimes_{11} \\ \vdots & & & & & & & & & & & & & \\ U_{11} \otimes_{11} & \otimes_{11}$$

eine nm×nm VBH-Matrix mit zugehörigen Submatrizen:

$$U_{i,j} \otimes V_{kl}$$
, $i \le i \le r$, $i \le j \le s$, $i \le k \le p$, $i \le l \le q$

Bew.: Die Unitarität der Matrix $\mathbf{U} \otimes_{\mathbf{g}} \mathbf{V}$ folgt z.B. aus der leicht nachzuprüfenden Existenz von nm×nm Permutationsmatrizen P und Q, sodaß gilt: $\mathbf{U} \otimes_{\mathbf{g}} \mathbf{V} = \mathbf{P}(\mathbf{U} \otimes \mathbf{V})\mathbf{Q}$ und der Unitarität von $\mathbf{U} \otimes \mathbf{V}$ als Tensorprodukt unitärer Matrizen.

Indem für bel.
$$4 \le i \le r$$
, $4 \le j \le s$, $4 \le k \le p$, $4 \le k \le q$ die bekannte Formel $\|\mathbf{U}_{i,j} \otimes \mathbf{V}_{kl}\|^2 = \|\mathbf{U}_{i,j}\|^2 \|\mathbf{V}_{kl}\|^2$

für die Hilbert-Schmidt-Norm gilt, folgt aus den entsprechenden Eigenschaften der Submatrizen von U und V, daß jene von U⊗_BV die Gleichung (1.5) erfüllen.

Ist v eine VH-Matrix (d.h. sind die Subblöcke $v_{i,j}$ alle ein-elementig), so ist offensichtlich: U⊗, V = U⊗V. Es liegt nahe von einem (verallgemeinerten) "Block-Tensorprodukt" zu sprechen.

Proposition 5.2 ist das Gegenstück zu Lemma 3.7: Sei die n×n VBH-Matrix \mathbf{U} zwei bzgl. $\frac{\mathbf{1}}{n}$ 1 unabhängigen, selbstadjungierten n×n Matrizen A und B und die m×m VBH-Matrix V zwei bzgl. $\frac{1}{m}$ 1 unabhängigen, selbstadjungierten m×m Matrizen C und D zugeordnet. Es ist leicht nachzuprüfen, daß dann U⊗ V (mit möglicherweise vergröberter Partition) eine den bzgl. 1 unabhängigen, selbstadj. nm×nm Matrizen A⊗C und B⊗D zugeordnete mn×mn VBH-Matrix ist.

Für die nun folgenden Konstruktionen beschränken wir uns der Einfachheit halber auf VH-Matrizen.

5.2. EINE KONSTRUKTION VON VH-MATRIZEN

Als Ausgangspunkt betrachten wir eine einfache Verallgemeinerung von Lemma 3.7, deren es eine ganze Reihe gibt.

Seien A und B zwei bzgl. 1 unabhängige, selbstadj. n×n Matrizen

mit kanonischer Spektralzerlegung:
$$A = \sum_{i=1}^r a_i P_i \qquad \text{und} \qquad B = \sum_{j=1}^s b_j \Omega_j$$

Seien weiters C_i , $1 \le i \le r$ und D_j , $1 \le j \le s$ selbstadj. $m \times m$ Matrizen, sodaß jedes beliebige Paar C_i und D_j mit $1 \le i \le r$, $1 \le j \le s$ unabhängig bzgl. $\frac{1}{m}$ 1 ist. Dann sind die mn×mn Matrizen: $E = \sum_{i=1}^{r} a_i P_i \otimes C_i \quad \text{und} \quad F = \sum_{j=1}^{s} b_j Q_j \otimes D_j$

$$E = \sum_{i=4}^{r} a_i P_i \otimes C_i$$
 und $F = \sum_{j=4}^{s} b_j Q_j \otimes D_j$

unabhängig bzgl. -11.

Der Beweis verläuft, indem man die kanonischen Spektralzerlegungen von C_i , $1 \le i \le r$ und D_i , $1 \le j \le s$ in E und F einsetzt, völlig analog wie Jener von Lemma 3.7.

Wir beschränken uns nun auf nichtentartete Matrizen A, B, C, ,i≤i≤n und D_i , $1 \le j \le n$ (r=s=n) und nehmen weiters an, daß auch E und F nichtentartet sind. Gesucht ist eine Formel für eine E und F zugeordnete mn×mn VH-Matrix.

Seien A und U-1BU diagonal, d.h. U die A und B zugeordnete n×n VH-Matrix. Seien weiters die unitären m×m Matrizen V_i, ≤i≤n bzw. W_i, $\overset{_{1}\leq_{j}\leq_{n}}{\text{so gewählt, daß }} V_{i}^{\overset{_{1}}{\text{c}}}C_{i}^{}V_{i}^{}, \ \overset{_{1}\leq_{i}\leq_{n}}{\text{bzw. }} \overset{_{w_{j}}^{-1}}{\text{D}_{j}}W_{j}^{}, \ \overset{_{1}\leq_{j}\leq_{n}}{\text{diagonal sind.}} C_{i}^{} \text{ und } D_{j}^{} \text{ sind für alle } \overset{_{1}\leq_{i}\leq_{n}}{\text{unabhängig bzgl.}} \overset{_{1}}{\overset{_{1}}{\text{m}}} 1 \text{ genau dann, wenn }$ die Matrizen V¼ für alle ₄≤i,j≤n m×m VH-Matrizen sind. Seien nun die nm×nm Matrizen: $V:=diag(V_1,...,V_p)$ bzw. $W:=diag(W_1,...,W_p)$. Es folgt, daß

 $V^{-1}EV$ und $W^{-1}(U^{-1}\otimes 1_{m})F(U\otimes 1_{m})W$

Diagonalmatrizen sind. Also sind E und F unabhängig bzgl. $\frac{1}{nm}$ 1 genau dann, wenn Z:=V⁻¹(U⊗1_)₩ eine nm×nm VH-Matrix ist. Zusammengefaßt:

5.3. Proposition: Sei U eine n×n VH-Matrix und seien \mathbf{V}_{i} , 1 $\leq i \leq n$ und ₩_j, ı≤j≤n unitäre m×m Matrizen, sodaβ V⁻¹_i, für alle ı≤i,j≤n jeweils m×m VH-Matrizen sind. Dann ist

$$Z := \begin{bmatrix} U_{11}V_{1}^{-1}W_{1} & U_{12}V_{1}^{-1}W_{2} & \dots & U_{1n}V_{1}^{-1}W_{n} \\ U_{21}V_{2}^{-1}W_{1} & U_{22}V_{2}^{-1}W_{2} & \dots & U_{2n}V_{2}^{-1}W_{n} \\ \vdots & \vdots & \ddots & \vdots \\ U_{n1}V_{n}^{-1}W_{1} & U_{n2}V_{n}^{-1}W_{2} & \dots & U_{nn}V_{n}^{-1}W_{n} \end{bmatrix}$$

eine nm×nm VH-Matrix

Bew.: -folgt aus der obigen Ableitung, indem Z die E und F zugeordnete VH-Matrix ist. Explizit sieht man die Unitarität von Z anhand der Zerlegung Z = V⁻¹(U⊗1_m)W, mit unitären V,W und U wie oben. Daβ die Einträge alle gleichen Absolutbetrag haben ist nach den Vor aussetzungen offensichtlich.

Prop. 5.3 ist also schnell direkt zu beweisen. Anhand der angebenen Ableitung lassen sich aber leichter Variationen bzw. Verallgemeinerungen, z.B. auf VBH-Matrizen, ableiten, wofür eine genauere Untersuchung aber noch aussteht.

Die Nützlichkeit des Ansatzes führen wir zuerst an Beispielen vor.

5.4. BEISPIELE:

i) Sei n=m=2. Sei U die bis auf Äquivalenz eindeutige 2×2 VH-Matrix, nämlich die 2×2 Fouriermatrix F(z). Sei nun $V_1=V_2=1$. Dann müssen nach Vorraussetzung W_1 und W_2 2×2 VH-Matrizen sein. Unter Vorwegnahme der Normalform von Z bleibt nur übrig $W_1=F(z)$ und $W_2=XF(z)$, mit $X={\rm diag}(1,e^{ix})$, $x\in[0,2\pi)$ zu setzen. Das ergibt:

$$Z_{x} = \sqrt{\frac{1}{2}} \begin{bmatrix} F_{(2)} & XF_{(2)} \\ F_{(2)} & -XF_{(2)} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & e^{ix} - e^{ix} \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -e^{ix} & e^{ix} \end{bmatrix}$$

Diese Matrizen werden durch Vertauschen der zweiten und dritten Spalte zu den Matrizen $\mathbf{U}_{\mathbf{x}}$ von Seite 9, von denen wir bereits bemerkten, daß sie für $\mathbf{x} \in [0,\pi/2]$ bis auf Äquivalenzen alle 4×4 VH–Matrizen sind.

ii) Sei n=2, m=3. Sei U=F(2), wie oben und $\mathbf{V_1}=\mathbf{V_2}=\mathbf{1}$. Also müssen $\mathbf{W_1}$ und $\mathbf{W_2}$ jeweils 3×3 VH-Matrizen sein. Da alle solchen Matrizen zu F(3) äquivalent sind, setzen wir analog zu oben $\mathbf{W_1}=\mathbf{F}(3)$ und $\mathbf{W_2}=\mathbf{YF}(3)$, mit $\mathbf{Y}=\mathrm{diag}(1,e^{ix},e^{iy})$, $\mathbf{x},\mathbf{y}\in[0,2\pi)$. Mit $\lambda=e^{i2\pi/3}$ erhalten wir:

$$Z_{xy} = \sqrt{\frac{1}{2}} \begin{bmatrix} F_{(3)} & YF_{(3)} \\ F_{(3)} & -YF_{(3)} \end{bmatrix} = \sqrt{\frac{1}{6}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \lambda & \lambda^2 & e^{ix} & \lambda e^{ix} & \lambda^2 e^{ix} \\ 1 & \lambda^2 & \lambda & e^{iy} & \lambda^2 e^{iy} & \lambda e^{iy} \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \lambda & \lambda^2 & -e^{ix} & -\lambda e^{ix} & -\lambda^2 e^{ix} \\ 1 & \lambda^2 & \lambda & -e^{iy} & -\lambda^2 e^{iy} & -\lambda e^{iy} \end{bmatrix}$$

Eine sorgfältige Analyse der Äquivalenzrelationen ergibt, daß alle Matrizen \mathbf{Z}_{xy} zu einer solchen mit $0 \le x \le \pi/3$, $0 \le y \le x/2$ äquivalent sind, auf welchem Definitionsbereich sie paarweise inäquivalent sind.

Der umgekehrte Ansatz mit n=3 und m=2, $\mathbf{V}=\mathbf{F}_{(3)}$, $\mathbf{V}_1=\mathbf{V}_2=\mathbf{V}_3=\mathbf{1}$ und \mathbf{W}_1 , \mathbf{W}_2 und \mathbf{W}_3 , die zu $\mathbf{F}_{(2)}$ äquivalent sind, liefert Matrizen, die alle zu den obigen äquivalent sind.

Im Gegensatz zu Punkt i) gibt es aber weitere inäquivalente Lösungen von Prop.5.3. Eine solche läßt sich leicht explizit angeben: Sei wieder n=2 und m=3, sowie V=F(z). Wir benützen nun die drei 3×3 VH-Matrizen mit Produkteigenschaft V_0 , V_1 und V_2 von Beispiel 4.18 und setzen $V_1=1$, $V_2=V_0$, $W_1=V_1$ und $V_2=V_2$. Die Vorraussetzung von Prop.5.3 sind damit offensichtlich erfüllt und wir erhalten, durch eine kurze Rechnung, als 6×6 VH-Matrix (mit $\lambda=e^{i2\pi/3}$):

$$Z_{\mathbf{B}} := \sqrt{2} \left[\begin{array}{cccc} \mathbf{U_{i}} & \mathbf{U_{2}} \\ \mathbf{U_{o}^{-i}U_{i}} & -\mathbf{U_{o}^{-i}U_{2}} \end{array} \right] = \sqrt{6} \left[\begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 & 1 \\ \lambda & \lambda^{2} & 1 & \lambda^{2} & 1 & \lambda \\ \lambda & 1 & \lambda^{2} & \lambda^{2} & \lambda & 1 \\ \lambda & 1 & \lambda^{2} & \lambda^{2} & \lambda & 1 \\ \vdots & \vdots \lambda^{2} & \vdots & \vdots \lambda & \vdots & \vdots \lambda \\ \vdots \lambda^{2} & \vdots & \vdots \lambda^{2} & \vdots & \vdots \lambda & \vdots & \vdots \lambda \\ \vdots \lambda^{2} & \vdots \lambda^{2} & \vdots & \vdots \lambda & \vdots \lambda & \vdots \end{array} \right]$$

Durch Multiplikation der Zeilen mit geeigneten Zahlen mit Absolutbetrag 1, erhalten wir als Normalform:

$$Z_{\mathbf{B}}' = \sqrt{s} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \lambda & \lambda^2 & \lambda & \lambda^2 & 1 \\ 1 & \lambda^2 & \lambda & \lambda & 1 & \lambda^2 \\ 1 & \lambda^2 & \lambda^2 & 1 & \lambda & \lambda \\ 1 & \lambda & 1 & \lambda^2 & \lambda & \lambda^2 \\ 1 & 1 & \lambda & \lambda^2 & \lambda^2 & \lambda \end{bmatrix}$$

Es ist leicht zu sehen, daß Z_{g}' zu keiner Matrix Z_{xy} von oben äquivalent ist. $\sqrt{s}Z_{g}'$ hat nur Einträge aus der Menge $\{1,\lambda,\lambda^2\}$, d.h. den dritten Einheitswurzeln und ist also eine H(3,6)-Matrix.

Die vollständige Bestimmung aller 6×6 VH-Matrizen ist ein noch offenes Problem. Im nächsten Abschnitt geben wir auch Lösungen an, die nicht entsprechend Prop.5.3 gebildet sind.

iii) Für höhere Ordnungen n,m erhält man so immmer umfangreichere Lösungen. Z.B. für n=2 und m=4 läßt sich sofort eine fünfparametrige Schar von 8×8 VH-Matrizen in Normalform angeben:

$$Z_{uvvxy} = \sqrt{\frac{1}{2}} \begin{bmatrix} Z_{x} & TZ_{y} \\ Z_{x} & -TZ_{y} \end{bmatrix}$$

mit den 4×4 VH-Matrizen Z_x und Z_y , wie oben und $T=diag(1,e^{iu},e^{iv},e^{iv})$, $u,v,v,s,y\in[0,2\pi)$, und es gibt noch weitere Lösungen dieser Ordnung.

Es ist also bereits für kleine n,m∈N schwer alle nm×nm Matrizen zu bestimmen, die entsprechend Prop.5.3 gebildet sind. Zwei spezielle Lösungen lassen sich, wie die Beispiele zeigen, explizit angeben.

Seien m,n>1, $\mathbf{U}=\mathbf{F}(n)$, $\mathbf{V_i}=\ldots=\mathbf{V_n}=\mathbf{1}$ und $\mathbf{W_i}=\mathbf{X_i}\mathbf{F}(m)$ mit unitären Diagonalmatrizen $\mathbf{X_i}$ für alle $\mathbf{1} \leq \mathbf{i} \leq n$. Dann sind die Vorraussetzungen von Prop. 5.3 erfüllt und wir erhalten mit $\lambda=e^{\mathbf{i}2\pi/n}$, als mn×mn VH-Matrix:

$$Z := \begin{bmatrix} X_1 F(m) & X_2 F(m) & \dots & X_n F(m) \\ X_1 F(m) & \lambda X_2 F(m) & \dots & \lambda^{-1} X_n F(m) \\ \vdots & & \vdots & & \vdots \\ X_1 F(m) & \lambda^{-1} X_2 F(m) & \dots & \lambda X_n F(m) \end{bmatrix}$$

oder mit $X := diag(X_1, ..., X_n)$ kurz:

$$Z = (F(n) \otimes 1_m) X (1_n \otimes F(m))$$
 (5.2)

Für die Normalform von Z müssen $X_i=1$ und die ersten Diagonaleinträge aller X_2,\ldots,X_n gleich 1 gesetzt werden. Die Phasen der restlichen Diagonaleinträge von X_2,\ldots,X_n sind noch (n-1)(m-1) freie Parameter.

Der Definitionsbereich der Parameter für paarweise inäquivalente Matrizen ist immer noch (n-1)(m-1)-dimensional, da die verbleibenden Äquivalenztransformationen eines normalisierten Z nur diskrete Operationen sind. Es folgt insbesondere, daß für jede Nichtprimzahlordnung unendlich viele inäquivalente VH-Matrizen existieren. Für Primzahlordnungen p lieferte Brock in [09] durch Angabe einer H(6,7)-Matrix auch das erste Beispiel einer pxp VH-Matrix, die nicht zur Fouriermatrix F(p) äquivalent ist. Weiteres ist nicht bekannt.

In Bsp.5.4 erhielten wir entsprechen Glchg.(5.2) die VH-Matrizen $\mathbf{Z}_{\mathbf{x}}$, bzw. $\mathbf{Z}_{\mathbf{xy}}$. Die 4×4 Matrix $\mathbf{Z}_{\mathbf{x}}$ wird für $\mathbf{x}=\pi/2$ und durch Vertauschen der zweiten und dritten Spalte zur Fouriermatrix $\mathbf{F}^{(4)}$. Die 6×6 Matrix $\mathbf{Z}_{\mathbf{xy}}$ wird für $\mathbf{x}=\mathbf{y}=\emptyset$ bei geeigneter Permutation von Zeilen und Spalten zur $\mathbf{F}^{(6)}$. Die Möglichkeit mittels Glchg.(5.2) für passendes \mathbf{X} und anschließender geeigneter Permutation von Zeilen und Spalten die nm×nm Fouriermatrix $\mathbf{F}^{(nm)}$ zu erhalten bildet (bei iterativer Anwendung) die Grundlage für die sogenannte "Schnelle Fouriertransformation" (FFT=Fast Fourier Transform -siehe Cooley/Tuckey [13]).

Butson's Definition verallgemeinerter Hadamard-Matrizen in [12] wurde durch die Entdeckung einer Formel für H(p,2p)-Matrizen (bzw. der daraus sofort folgenden Existenz von $H(p,2^mp^k)$ -Matrizen für $m \le k$) für bel. Primzahlen p veranlaßt. Für p=2 ist H(2,4) die 4×4 Hadamard-Matrix. Für p=3 wurde eine H(3,6)-Matrix: $\sqrt{a}Z_B'$ in Beispiel 5.4.ii) abgeleitet. Dieser Zugang liefert für alle Primzahlen p>2 Butson'sche H(p,2p)-Matrizen, wie wir nun kurz skizzieren:

Seien $\mathbf{X_a}$, $\mathbf{a} \in \mathbf{F_q}$ die $\mathbf{q} \times \mathbf{q}$ VH-Matrizen mit Produkteigenschaft von Korollar 4.17 für eine bel. ungerade Primzahlpotenz $\mathbf{q} = \mathbf{p}^m$, $\mathbf{m} \in \mathbb{N}$. Wir benötigen eigentlich nur $\mathbf{q} = \mathbf{p} > 2$, doch gilt das Folgende allgemein. Es ist unter Verwendung von Theorem 5.15 über Gaussummen und Theorem 5.33 aus Lidl/Niederreiter [31] leicht zu zeigen, daß für die VH-Matrizen $\mathbf{X_a^{-1}X_b}$ mit $\mathbf{a} \neq \mathbf{b} \in \mathbf{F_q}$ gilt:

$$X_a^{-1}X_b = \alpha(q)\eta(b-a)Y_{ab}$$

wobei $\alpha(q)$ eine komplexe Zahl mit Absolutbetrag 1 ist, die nur von q (und dem für die Bildung von $\mathbf{X_a}$ und $\mathbf{X_b}$ verwendeten nichttrivialen, additiven Charakter) abhängt. η ist der sogenannte quadratische Charakter: $\eta(\mathbf{c})=1$, falls \mathbf{c} Quadrat eines Elementes von $\mathbf{F_q}$ ist, sonst ist $\eta(\mathbf{c})=-1$. $\mathbf{Y_{ab}}$ ist eine von \mathbf{a} und \mathbf{b} abhängige Matrix, der Art, daß $\sqrt{\mathbf{q}}\mathbf{Y_{ab}}$ (wie auch jedes $\sqrt{\mathbf{q}}\mathbf{X_a}$) nur p-te Einheitswurzeln als Einträge hat.

Seien die Matrizen U=F(2), $V_1=1_q$, $V_2=X_o$, $W_1=X_1$ und $W_2=X_c$, mit einem nichtquadratischen Element $c \in F_q$. Die Vorraussetzungen von Prop.5.3 sind damit erfüllt und wir erhalten als 2q×2q VH-Matrix:

$$Z_{\mathbf{B}} = \sqrt{2} \begin{bmatrix} X_{\mathbf{i}} & X_{\mathbf{C}} \\ X_{\mathbf{O}}^{-1} X_{\mathbf{i}} & -X_{\mathbf{O}}^{-1} X_{\mathbf{C}} \end{bmatrix}$$

Es gilt:

$$\begin{split} &X_{o}^{-i}X_{i} = \alpha(q)\eta(i)Y_{oi} = \alpha(q)Y_{oi} \\ &X_{o}^{-i}X_{c} = \alpha(q)\eta(c)Y_{oc} = -\alpha(q)Y_{oc} \end{split}$$

Also wird $\mathbf{Z_{B}}$ durch Multiplikation der unteren q Zeilen mit $\overline{\alpha}(\mathbf{q})$ zu:

$$Z'_{B} = \frac{i}{\sqrt{2}} \begin{bmatrix} X_{i} & X_{C} \\ Y_{Oi} & Y_{OC} \end{bmatrix}$$

und $\sqrt{2q}Z_B'$ ist eine $H(p,2q)=H(p,2p^m)-Matrix, meN.$

5.3. PRODUKTE

Es soll noch eine Konstruktion von Paaren von VH-Matrizen $\mathbf{Z_i}$ und $\mathbf{Z_2}$ mit Produkteigenschaft, d.h. für die auch $\mathbf{Z_i^{-1}Z_2}$ eine VH-Matrix ist, angegeben werden, welche das Beispiel von Seite 12 verallgemeinert.

Sei F(m) die m×m Fouriermatrix und seien U,V,X und Y jeweils unitäre m×m Diagonalmatrizen: U=diag($e^{iU_1}, \dots e^{iU_m}$), V=diag($e^{iV_1}, \dots , e^{iV_m}$), X=diag($e^{iX_1}, \dots , e^{iX_m}$), Y=diag($e^{iY_1}, \dots , e^{iY_m}$), mit u_i,V_i,X_i,Y_i \in [0,2 π) für alle $_{1 \le i \le m}$. Dann sind

$$Z_{\underline{1}} := \sqrt{\frac{1}{2}} \begin{bmatrix} F(m) & XF(m) \\ & & \\ F(m) & -XF(m) \end{bmatrix} \qquad Z_{\underline{2}} := \sqrt{\frac{1}{2}} \begin{bmatrix} UF(m) & UYF(m) \\ & & \\ VF(m) & -VYF(m) \end{bmatrix}$$
(5.3)

beides $2m\times 2m$ VH-Matrizen. Die Äquivalenzrelationen vorwegnehmend ist die erste Spalte von Z_1 bereits normiert. Für die erste Spalte von Z_2 ist das gleichzeitig nicht mehr möglich (siehe Bemerkung im Anschluß an Def. 3.2'). Z_1 und $Z_2' = \left(\text{diag}(\mathbf{U}^{-1}, \mathbf{V}^{-1})\right)Z_2$ sind offensichtlich entsprechend Glchg. (5.2) gebildet.

Wir wollen die Produkte $\mathbf{Z_1^{-1}Z_2}$ untersuchen. Dazu benötigen wir:

5.5. LEMMA: Eine komplexe 2×2 Matrix M ist unitär genau dann, wenn es $u,v,x,y\in[0,2\pi)$ gibt, sodaß gilt:

$$\mathbf{M} = \mathbf{M}(\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}) = \frac{1}{2} \begin{bmatrix} (e^{\mathbf{i}\mathbf{u}} + e^{\mathbf{i}\mathbf{v}}) & e^{\mathbf{i}\mathbf{y}} (e^{\mathbf{i}\mathbf{u}} - e^{\mathbf{i}\mathbf{v}}) \\ e^{-\mathbf{i}\mathbf{x}} (e^{\mathbf{i}\mathbf{u}} - e^{\mathbf{i}\mathbf{v}}) & e^{-\mathbf{i}\mathbf{x}} e^{\mathbf{i}\mathbf{y}} (e^{\mathbf{i}\mathbf{u}} + e^{\mathbf{i}\mathbf{v}}) \end{bmatrix}$$

Bew.: Für alle u,v,x,y∈[0,2π) ist

$$\mathbf{M}(\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\mathbf{x}} \end{bmatrix} \mathbf{v}_{\mathbf{z}}^{\mathbf{i}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} e^{i\mathbf{u}} & 0 \\ 0 & e^{i\mathbf{v}} \end{bmatrix} \mathbf{v}_{\mathbf{z}}^{\mathbf{i}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\mathbf{y}} \end{bmatrix}$$

als Produkt von fünf unitären Matrizen unitär.

Sei umgekehrt

$$\mathbf{M} = \left[\begin{array}{cc} \mathbf{a} & \mathbf{c} \\ \mathbf{b} & \mathbf{d} \end{array} \right]$$

eine beliebige unitäre 2×2 Matrix. M*=M-1 ergibt explizit:

$$\begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} = \frac{1}{ad-bc} \begin{bmatrix} d - c \\ -b & a \end{bmatrix}$$

Die Determinante einer unitären Matrix hat Absolutbetrag 1. Sei also ad-bc = $\mathrm{e}^{\mathrm{i}\eta}$, mit η =[0,2 π)

$$\Rightarrow M = \begin{bmatrix} a & -e^{i\eta}\overline{b} \\ b & e^{i\eta}\overline{a} \end{bmatrix}$$

wobei $|a|^2 + |b|^2 = 1$ gelten muß. Also gibt es $\alpha, \beta \in [0, 2\pi)$ und $\gamma \in [0, \pi/2]$, sodaß: $a = e^{i\alpha} \cos(\gamma)$ und $b = e^{i\beta} \sin(\gamma)$

Setzen wir nun z.B.: u,v,x,y∈[0,2π) modulo 2π gleich:

$$U=\alpha+\gamma$$
, $V=\alpha-\gamma$, $\chi=\alpha-\beta+\pi/2$, $y=\eta-\beta-\alpha+\pi/2$,

Dann folgt leicht:

$$a = \frac{1}{2}(e^{iU} + e^{iV}) \qquad -e^{i\eta}\overline{b} = \frac{1}{2}e^{iy}(e^{iU} - e^{iV})$$

$$b = \frac{1}{2}e^{-ix}(e^{iU} - e^{iV}) \qquad e^{i\eta}\overline{a} = \frac{1}{2}e^{-ix}e^{iy}(e^{iU} + e^{iV})$$

und oben eingesetzt M = M(u, v, x, y).

Es ist einfach nachzuprüfen, daß u,v,x,y \in [0,2 π) eindeutig festgelegt sind bis auf: \mathbf{M} (u,v,x,y)= \mathbf{M} (v,u,x+ π ,y+ π), \mathbf{M} (u,u,x,y)= \mathbf{M} (u,u,x+w,y+w) und \mathbf{M} (u,u+ π ,x,y)= \mathbf{M} (u+w,u+w+ π ,x+w,y-w) für bel.w \in [0,2 π).

Erinnert sei nun noch an die Definition von zirkulanten Matrizen:

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{bmatrix}$$

Das sind jene Matrizen A, bei denen die Elemente jeder Reihe identisch sind mit denen der vorhergehenden Reihe, aber um eine Stelle zyklisch nach rechts verschoben.

5.6. PROPOSITION:

Eine 2m×2m Matrix
$$T = \begin{bmatrix} A & C \\ B & D \end{bmatrix}$$

-ist unitär und hat zirkulante m×m Submatrizen A,B,C und D genau dann, wenn es 2m×2m VH-Matrizen Z_1 und Z_2 entsprechend Glchg.(5.3) gibt, sodaß $T = Z_1^{-1}Z_2$ gilt.

Beweis: Seien die 2m×2m VH-Matrizen $\mathbf{Z_i}$ und $\mathbf{Z_2}$ wie in (5.3) gegeben. Dann ist $\mathbf{Z_i^{-1}Z_2}$ als Produkt unitärer Matrizen unitär und zwar:

$$Z_{\underline{1}}^{-\underline{1}}Z_{\underline{2}} \; = \; \frac{1}{2} \left[\begin{array}{ccc} F_{\text{(m)}}^{-\underline{1}} \left(U + V \right) F_{\text{(m)}} & F_{\text{(m)}}^{-\underline{1}} \left(Y \left(U - V \right) \right) F_{\text{(m)}} \\ F_{\text{(m)}}^{-\underline{1}} \left(X^{-\underline{1}} \left(U - V \right) \right) F_{\text{(m)}} & F_{\text{(m)}}^{-\underline{1}} \left(X^{-\underline{1}} Y \left(U + V \right) \right) F_{\text{(m)}} \end{array} \right]$$

Die Matrizen (U+V), Y(U-V), $X^{-1}(U-V)$ und $X^{-1}Y(U+V)$ sind ebenso wie U,V,X und Y diagonal und es ist wohlbekannt (siehe z.B. Davis [16], Theorem 3.2.3), daß für jede beliebige m×m Diagonalmatrix N gilt, daß $F(m)^{-1}NF(m)$ eine zirkulante Matrix ist.

Sei nun umgekehrt

$$T = \left[\begin{array}{cc} A & C \\ B & D \end{array} \right]$$

eine beliebige unitäre 2m×2m Matrix mit zirkulanten m×m Submatrizen A,B,C und D. Zu jeder zirkulanten m×m Matrix A existiert (wie wieder wohlbekannt, siehe Davis [16], Theorem 3.2.2) eine m×m Diagonalmatrix A, sodaß $A = F(m)^{-1}AF(m)$ gilt. Sei also

$$T \ = \ \begin{bmatrix} \mathbf{F} \cdot \mathbf{m} \rangle^{\mathbf{1}} \mathbf{\tilde{A}} \mathbf{F} \cdot \mathbf{m} \rangle & \mathbf{F} \cdot \mathbf{m} \rangle^{\mathbf{1}} \mathbf{\tilde{C}} \mathbf{F} \cdot \mathbf{m} \rangle \\ \mathbf{F} \cdot \mathbf{m} \rangle^{\mathbf{1}} \mathbf{\tilde{B}} \mathbf{F} \cdot \mathbf{m} \rangle & \mathbf{F} \cdot \mathbf{m} \rangle^{\mathbf{1}} \mathbf{\tilde{C}} \mathbf{F} \cdot \mathbf{m} \rangle \end{bmatrix} \ = \ \begin{bmatrix} \mathbf{F} \cdot \mathbf{m} \rangle^{\mathbf{1}} & 0 \\ 0 & \mathbf{F} \cdot \mathbf{m} \rangle^{\mathbf{1}} \end{bmatrix} \begin{bmatrix} \mathbf{\tilde{A}} & \mathbf{\tilde{C}} \\ \mathbf{\tilde{B}} & \mathbf{\tilde{D}} \end{bmatrix} \begin{bmatrix} \mathbf{\tilde{F}} \cdot \mathbf{m} \rangle & 0 \\ 0 & \mathbf{F} \cdot \mathbf{m} \rangle \end{bmatrix}$$

 $\begin{array}{ll} \text{mit $\tilde{\mathbf{A}}$=} \text{diag}(a_{\underline{\mathbf{a}}},\ldots,a_{\underline{\mathbf{m}}}) \;,\;\; \tilde{\mathbf{B}}$=} \text{diag}(b_{\underline{\mathbf{a}}},\ldots,b_{\underline{\mathbf{m}}}) \;,\;\; \tilde{\mathbf{C}}$=} \text{diag}(c_{\underline{\mathbf{a}}},\ldots,c_{\underline{\mathbf{m}}}) \;\; \text{und } \\ \tilde{\mathbf{D}}$=} \text{diag}(d_{\underline{\mathbf{a}}},\ldots,d_{\underline{\mathbf{m}}}) \;,\;\; a_{\underline{\mathbf{k}}},b_{\underline{\mathbf{k}}},c_{\underline{\mathbf{k}}},d_{\underline{\mathbf{k}}} \in \mathbb{C} \;\; \text{für alle } \underline{\mathbf{a}} \leq \underline{\mathbf{k}} \leq \underline{\mathbf{m}} \;.\;\; \text{Seien} \end{array}$

$$\mathbf{S}_{\mathbf{k}} := \left[\begin{array}{cc} \mathbf{a}_{\mathbf{k}} & \mathbf{C}_{\mathbf{k}} \\ \mathbf{b}_{\mathbf{k}} & \mathbf{d}_{\mathbf{k}} \end{array} \right] \qquad \text{für } \mathbf{1} \leq \mathbf{k} \leq \mathbf{m}$$

Man sieht sofort, daß T genau dann unitär ist wenn S_k für alle $1 \le k \le m$ unitäre 2×2 Matrizen sind. Mit Lemma 5.5 folgt, daß für alle $1 \le k \le m$ U_k , V_k , V_k , V_k , V_k V_k V_k , V_k V_k V_k , V_k , V

$$S_k = M(u_k, v_k, x_k, y_k)$$
 für $4 \le k \le m$

Sei nun unitäre m×m Matrizen ∪,∨,X und Y definiert durch:

$$\begin{aligned} & \mathbf{V} = \operatorname{diag}(e^{\mathsf{i} \mathsf{V}_{\mathbf{1}}}, \dots, e^{\mathsf{i} \mathsf{V}_{\mathbf{m}}}) & \mathbf{V} = \operatorname{diag}(e^{\mathsf{i} \mathsf{V}_{\mathbf{1}}}, \dots, e^{\mathsf{i} \mathsf{V}_{\mathbf{m}}}) \\ & \mathbf{X} = \operatorname{diag}(e^{\mathsf{i} \mathsf{X}_{\mathbf{1}}}, \dots, e^{\mathsf{i} \mathsf{X}_{\mathbf{m}}}) & \mathbf{Y} = \operatorname{diag}(e^{\mathsf{i} \mathsf{Y}_{\mathbf{1}}}, \dots, e^{\mathsf{i} \mathsf{Y}_{\mathbf{m}}}) \end{aligned}$$

Dann folgt sofort:

$$\mathring{A} = \frac{1}{2}(U+V)$$
, $\mathring{B} = \frac{1}{2}X^{-1}(U-V)$, $\mathring{C} = \frac{1}{2}Y(U-V)$ und $\mathring{D} = \frac{1}{2}X^{-1}Y(U+V)$

und die mit diesen $\mathbf{U},\mathbf{V},\mathbf{X},\mathbf{Y}$ entsprechend (5.3) gebildeten $\mathbf{Z_i}$ und $\mathbf{Z_2}$ erfüllen $\mathbf{Z_i^{-1}Z_2} = \mathbf{T}$

Das Problem alle $2m\times 2m$ VH-Matrizen $\mathbf{Z_1}$ und $\mathbf{Z_2}$ von Glchg. (5.3) mit Produkteigenschaft zu bestimmen ist also äquivalent dazu alle $2m\times 2m$ VH-Matrizen \mathbf{T} mit zirkulanten $m\times m$ Submatrizen (wie oben) zu bestimmen. Die Beweise von Prop.5.6 und Lemma 5.5 geben dann sogar einen expliziten Konstruktionsweg für die zugehörigen $\mathbf{Z_1}$ und $\mathbf{Z_2}$ an, wobei diese aber nur insoweit festgelegt sind, als es die $\mathbf{M}(\mathbf{u_k}, \mathbf{v_k}, \mathbf{x_k}, \mathbf{y_k})$ für $1 \le k \le m$ (siehe oben) sind.

5.7. BEISPIELE:

- i) Für m=2 entsprechen dem die Lösungen von Seite 12. Die dort angegebenen Matrizen $\mathbf{U}_{\mathbf{x}}$ und $\mathbf{V}_{\mathbf{yz}}$, $\mathbf{x}.\mathbf{y}.\mathbf{z} \in [0,2\pi)$ werden durch Vertauschen der jeweiligen zweiten und dritten Spalte zu $\mathbf{Z}_{\mathbf{i}}$ und $\mathbf{Z}_{\mathbf{z}}$ wie oben und $\mathbf{U}_{\mathbf{x}}^{-\mathbf{i}}\mathbf{V}_{\mathbf{yz}}$ wird bei Vertauschen der zweiten und dritten Spalte und Zeile zu einer 4×4 VH-Matrix mit zirkulanten 2×2 Submatrizen. Dies sind (wie eine längere explizite Überprüfung zeigt) bis auf Äquivalenzen bereits alle Paare von 4×4 VH-Matrizen mit Produkteigenschaft.
- ii) Für m=3 konnten bislang (bis auf Äquiv.) nur die folgenden 6×6 VH-Matrizen mit zirkulanten 3×3 Submatrizen gefunden werden:

$$T_{x} = \sqrt{\frac{1}{6}} \begin{bmatrix} 1 & -e^{-ix} & e^{ix} & -1 & ie^{-ix} & ie^{ix} \\ e^{ix} & 1 & -e^{-ix} & ie^{ix} & -1 & ie^{-ix} \\ -e^{-ix} & e^{ix} & 1 & ie^{-ix} & ie^{ix} & -1 \\ \hline 1 & ie^{-ix} & ie^{ix} & 1 & e^{-ix} & -e^{ix} \\ ie^{ix} & 1 & ie^{-ix} & 1 & e^{-ix} & -e^{ix} \\ ie^{-ix} & ie^{ix} & 1 & e^{-ix} & -e^{ix} & 1 \end{bmatrix} \quad x \in [0, 2\pi)$$

Wir verzichten darauf, zugeordnete $\mathbf{Z_i}^{\infty}$ und $\mathbf{Z_2}^{\infty}$ explizit anzugeben, da deren Einträge i.A. komplizierte trigonometrische Funktionen von x sind. Speziell sind unter den so erhaltenen unendlich vielen Paaren von 6×6 VH-Matrizen mit Produkteigenschaft auch Lösungen, die zu den zwei Matrizen $\mathbf{U_i}$ und $\mathbf{U_2}$ von Lemma 4.20, bzw. den von Korollar 4.21 für die Ordnung 6 gelieferten äquivalent sind. Alle $\mathbf{T_x}$ sind zu solchen mit x \in [0, π /12] äquivalent, auf welchem Definitionsbereich sie paarweise inäquivalent sind. Sie sind inäquivalent zu allen in Bsp.5.4.ii) angegebenen 6×6 VH-Matrizen.

Die VH-Matrizen T_{x} , von oben sind speziell von von der Gestalt:

mit zirkulanten Submatrizen A und B. Turyn zeigte, daß zu jeder 2m×2m VH-Matrix T dieser Form, für die 12mT eine H(4,2m)-Matrix (d.h. eine komplexe Hadamard-Matrix) ist, eine 4m×4m gewöhnliche Hadamard-Matrix von sogenanntem Williamson-Typ (Williamson [50]) korrespondiert (siehe Wallis [46], Theorem 6.4). Zum Beispiel ist 16T° von oben eine H(4,6)-Matrix, welcher sich so eine 12×12 Williamson-Hadamard-Matrix zuordnen läßt. Mittels dieses Zugangs gelang es Turyn [44] erstmals eine unendliche Familie von Hadamard-Matrizen des Williamson-Typs zu konstruieren.

Die Matrizen \mathbf{Z}_{xy} , $0 \le x \le \pi/3$, $0 \le y \le x/2$ und $\mathbf{Z}_{\mathbf{B}}$ von Beispiel 5.4.ii), sowie $\mathbf{T}_{\mathbf{x}}$, $0 \le x \le \pi/12$. von Beispiel 5.7.ii) sind die bis auf Äquivalenzen einzigen explizit bekannten 6×6 VH-Matrizen. Auch die Suche nach $\mathbf{H}(\mathbf{k},6)$ -Matrizen für kleine $\mathbf{k} \in \mathbb{N}$ mittels Computer lieferte keine weiteren Lösungen. Die jedem $\mathbf{T}_{\mathbf{x}}$, $\mathbf{x} \in [0,2\pi)$ zugeordneten 6×6 VH-Matrizen $\mathbf{Z}_{\mathbf{1}}^{(\omega)}$ und $\mathbf{Z}_{\mathbf{2}}^{(\omega)}$ sind die bis auf Äquivalenzen einzigen bekannten Paare von 6×6 VH-Matrizen mit Produkteigenschaft.

Auf Basis dieser Ergebnisse konnte bislang keinerlei Hinweis auf Tripel von VH-Matrizen mit Produkteigenschaft gefunden werden, was Anlaß gibt zu:

5.8. VERMUTUNG:

Es gibt keine drei 6x6 VH-Matrizen mit Produkteigenschaft.

Das kann als Gegenstück zur schon von L.Euler vermuteten und erst in unserem Jahrhundert bewiesenen Nichtexistenz von zwei orthogonalen Lateinischen 6×6 Quadraten interpretiert werden. Diese ist äquivalent dazu, daß es keine vier kommutierende 36×36 Matrizen mit jeweils 6 verschiedenen Eigenwerten gibt, die unabhängig bzgl. $\frac{1}{36}$ 1 sind. Obige Vermutung ist äquivalent dazu, daß es keine vier nicht-kommutierende 6×6 Matrizen mit jeweils 6 verschiedenen Eigenwerten (nichtentartet) gibt, die unabhängig bzgl. $\frac{1}{6}$ 1 sind. In beiden Fällen würde eine vollständige Lösung sieben derartige Matrizen umfassen.

6. ANWENDUNGEN

Als erstes zeigen wir wie sich aus den Lösungen von Kap.4 interessante Beispiele zu der folgenden Problemstellung konstruieren lassen. Unsere Terminologie orientiert sich an Busch/Lahti [11].

- 6.1 DEFINITION: Sei ≠ eine Menge von selbstadjungierten Operatoren über einem komplexen, separablen Hilbertraum औ.
- i) Zwei Dichteoperatoren (siehe Kap.2) D, ,D,∈D über % heißen 4äquivalent, falls für alle Operatoren A∈∅ und Borelmengen B⊆R gilt: $tr(D_{\lambda_n}(A)) = tr(D_{\lambda_n}(A))$
- ii) ₰ heißt "informationsvollständig", falls aus der ₰-Äquivalenz zweier beliebiger Dichteoperatoren $D_1, D_2 \in \mathcal{D}$ folgt: $D_1 = D_2$. iii) ≰ heiβt "informationsvollständig bzgl. den reinen Zuständen" (=orthogonale Projektionsoperatoren auf eindim. Teilräume: D=P_, siehe Kap.2), falls aus der ≪-Äquivalenz beliebiger P,P,∈⊅ folgt:

P=P, d.h. $e=\lambda f$ mit $\lambda \in \mathbb{C}$, $|\lambda|=1$.

Die physikalische Motivation der Definition ist offensichtlich: Zwei 4-äquivalente Zustände D, und D, lassen sich auch durch wiederholte, statistische Messungen der Werte der Observablen A∈ฬ (an identischen Systemen) nicht unterscheiden. Für die (zumindest prinzipielle Möglichkeit der) eindeutigen Bestimmung (bzw. Rekonstruktion) des Zustands durch Messungen sind informationsvollständige Mengen von Observablen notwendig.

Speziell untersucht wurden bislang, zurückreichend auf eine Anre gung von Wolfgang Pauli aus dem Jahre 1933, vor allem die, wie viele Beispiele zeigen, bzgl. reinen Zuständen nicht informationsvollständige Menge A={X,P} und diverse Erweiterungen davon (siehe z.B. Vogt [45], Corbett/Hurst[14] und Wiesbrock [49]) und im \mathbb{C}^n die Mengen der Spin-observablen (siehe z.B. Stulpe/Singer [42], Singer/Stulpe [40]).

Wir beschränken uns nun auf endlichdimensionale Hilberträume. Sei %=Cⁿ und ℐ={A: i∈I} eine Menge von komplexen, selbstadj. n×n Matrizen (mit Indexmenge I). Seien deren kanon. Spektralzerlegungen: $\mathbf{A}_i = \sum_{k=1}^{r~(i)} a_k^{(i)} P_k^{(i)} \quad \text{für alle } i{\in}\mathbf{I}$

$$A_i = \sum_{k=1}^{r(i)} a_k^{(i)} P_k^{(i)}$$
 für alle i \in I

mit den jeweils verschiedenen Eigenwerten $a_k^{(i)}$ und assoz. Proj. $P_k^{(i)}$, $a \le k \le r$ für alle $i \in I$. Es folgt sofort, daß zwei n×n Dichtematrizen D_1 und D_2 A-äquivalent sind, genau dann wenn gilt:

$$\operatorname{tr}(D_{\underline{\mathbf{1}}}P_{k}^{(i)}) \; = \; \operatorname{tr}(D_{\underline{\mathbf{2}}}P_{k}^{(i)}) \quad \text{für alle } i{\in}I \; , \; \underline{\mathbf{1}}{\leq}k{\leq}\mathrm{r}(i)$$

Busch und Lahti zeigen (in [11], im Beweis von Theorem 2.5.1), daß eine Menge $\mathscr{A}=\{A_i: i\in I\}$ von selbstadj. nxn Matrizen informationsvollständig ist, genau dann wenn die Spektralprojektionen $P_k^{(i)}$, $i\in I$, $1\le k\le r(i)$ den ganzen n^2 -dimensionalen Vektorraum M_n der komplexen $n\times n$ Matrizen aufspannen.

Für die Informationsvollständigkeit bzgl. reinen Zuständen ist hingegen keine solche eindeutige Charakterisierung bekannt.

Es gibt z.B. bzgl. reinen Zuständen sowohl informationsvollständige als auch -unvollständige Mengen ≠ von selbstadj. n×n Matrizen, wo die Spektralproj. der A einen (n²-1)-dimensionalen Teilraum von M aufspannen. Beispiele dafür lassen sich etwa aus den vollständigen Lösungen von paarweise bzgl. 1 unabhängigen, selbstadj. n×n Matrizen konstruieren, indem zwei verschiedene Eigenwerte einer beliebigen Matrix gleichgesetzt werden. Ohne Beweis sei erwähnt, daß man so ausgehend von den Lösungen von Satz 4.5 bzgl. reinen Zuständen nichtinformationsvollständige, ausgehend von Bsp.4.10 für ≥2 bzgl. reinen Zuständen informationsvollständige Mengen erhält.

Dies zeigt insbesondere, daß aus der Informationsvollständigkeit bzgl. reinen Zuständen nicht die allgemeine Informationsvollständigkeit folgt (siehe Fragestellung in Busch/Lahti [11], p.639/641), aber auch, daß z.B. die Dimension des von den Spektralprojektionen der $\mathbf{A}_{i} \in \mathcal{A}$ aufgespannten Teilraums von \mathbf{M}_{n} nicht genügt um die Informationsvollständigkeit bzgl. reinen Zuständen zu charakterisieren. Dazu benötigt es weiterer Kriterien.

Ein solches wurde etwa von Moroz [34] vorgeschlagen, der vermutete, daß es ein m≥4 gibt, sodaß jede Menge $\mathscr{A}=\{A_1,\ldots,A_m\}$ von m selbstadj. Operatoren über einem beliebigen separablen Hilbertraum $\mathscr R$ informationsvollständig bzgl. den reinen Zuständen ist (bzw. "hinreichend" nach Moroz), falls A_i und A_j für bel. $1 \le i \ne j \le m$ jeweils keinen gemeinsamen invarianten, nichttrivialen Unterraum haben.

Für unendlichdimensionale ೫ wurde dies bereits durch eine Arbeit von Wiesbrock [49] wiederlegt.

Ein einfaches Gegenbeispiel im \mathbb{C}^n erhalten wir ausgehend von der vollständigen Menge $\mathscr{A}=\{A_0,\dots,A_q\}$ von q+1 paarweise bzgl. $\frac{1}{q}$ 1 unabhängigen, selbstadjungierten, nichtentarteten q×q Matrizen, die es nach Satz 4.5 für bel. Primzahlpotenzen q gibt. Lassen wir eine der Marizen, etwa A_0 , weg und setzen wir $\mathscr{A}'=\{A_1,\dots,A_q\}$. Es ist leicht zu sehen, daß \mathscr{A}' , für beliebig große q, die Vorraussetzung der Hypothese von Moroz erfüllt. \mathscr{A}' ist aber nicht informationsvollständig bzgl. den reinen Zuständen: z.B. sind die q eindimensionalen Spektralprojektionen von A_0 : $P_k^{(0)}$, $1 \le k \le q$ alle \mathscr{A}' -äquivalent, da gilt:

$$tr(P_k^{(0)}P_l^{(i)}) = \frac{i}{q} \text{ für alle } i \le i,k,l \le q.$$

Dieses Beispiel ist auch interessant im Vergleich zur klassischen Wahrscheinlichkeitstheorie, wo bereits zwei (bzgl. der Gleichverteilung unabhängige) Zufallsvariablen $\mathbf{f_1},\mathbf{f_2}$ über $\Omega = \{\omega_{ij}: \mathbf{1} \leq i \leq p, \mathbf{1} \leq j \leq q\}$ der Gestalt $\mathbf{f_1}(\omega_{ij}) = \mathbf{g_1}(i)$ und $\mathbf{f_2}(\omega_{ij}) = \mathbf{g_2}(j)$, wobei die Werte $\mathbf{g_1}(i)$, $\mathbf{1} \leq i \leq p$ und $\mathbf{g_2}(j)$, $\mathbf{1} \leq j \leq q$ jeweils verschieden seien, informationsvollständig bzgl. den reinen Zuständen (=Punktmaßen μ) sind.

Dies berechtigt zu sagen, daß die reinen Zustände in der Quantenwahrscheinlichkeitstheorie mehr Information enthalten, als jene in der klassischen Wahrscheinlichkeitstheorie.

Noch eine kurze abschließende Bemerkung:

Die Unabhängigkeit bzgl. dem (normierten) Einheitsoperator von zwei selbstadjungierten Operatoren über einem separablen Hilbertraum $\mathscr R$ umfaßt auch physikalisch signifikante Lösungen: Paare $A\otimes 1$ und $1\otimes B$ (siehe Satz 3.6 für endlichdim. $\mathscr R$, Bsp. 2.12 für unendlichdim. $\mathscr R$) beschreiben quantenmechanisch völlig unabhängige Observablen. Zu dem kanonisch konjugierten Paar X und P über $\mathscr E^2(\mathbb R)$ (siehe Prop. 2.13) korrespondieren klassisch unabhängige Observablen.

Da die Unabhängigkeit eine grundlegende Kategorie in jeglicher Beschreibung der Wirklichkeit ist, wäre die Bestimmung aller Lösungen von (im besonderen bgl. $\frac{1}{n}$ 1 bzw. 1) unabhängigen Observablen in der Quantenmechanik von prinzipiellem Interesse. Dies könnte auch weitere Anwendungen zum Vorschein bringen.

Literaturverzeichnis

- [01] ACCARDI, L.: Some trends and problems in quantum probability in: Accardi, L. et.al. (eds.): Qu. Prob. and Appl. to the Qu. Th. of Irrev. Proc. LNM. 1055 Springer, Berlin-Heidelberg-N.Y. (1984)
- [02] AGAIAN, S.S.: Hadamard Matrices and Their Applications, LNM 1168, Springer-Verlag, Berlin-Heidelberg-N.Y. (1985)
- [03] AMREIN, W.O. und BERTHIER, A.M.: On support properties of L^p-functions and their Fourier transforms, J. Funct. Anal. 24, 258-267 (1977)
- [04] AUSLANDER, L. und TOLIMIERI, R.: Is computing with the finite Fourier transform pure or applied mathematics? Bull. Amer. Math. Soc. (New Ser.) 1, 847-897 (1979)
- [05] BAUER, H.: Wahrscheinlichkeitstheorie und Grundzüge der Maßtheorie, Walter de Gruyter, Berlin-New York (1978)
- [06] BELTRAMETTI, E.G. und CASINELLI, G.: The Logic of Quantum Mechanics, Addison-Wesley, Reading, Massachusetts (1981)
- [07] BETH, Th. JUNGNICKEL, D. und LENZ, H.: Design Theory, B.I. Mannheim-Wien-Zürich (1985)
- [08] BOSE, R.C. und BUSH, K.A.: Orthogonal Arrays of Strength two and three, Ann. Math. Stat. 23, 508-524 (1952)
- [09] BROCK, B.W.: Hermitian Congruence and the Existence and Completion of Generalized Hadamard Matrices, J. Comb. Theor. Ser. A 49, 233-261 (1988)
- [10] BUB, J.: Conditional probabilities in non-Boolean possibility structures, in: Hooker, C.A. (ed.): The Logico-Algebraic Approach to Quantum Mechanics II, Reidel, Dordrecht (1979)
- [11] BUSCH, P. und LAHTI, P.J.: The Determination of the past and the future of a physical system in quantum mechanics, Found. Phys. 19, 633-678 (1989)
- [12] BUTSON, A.T.: Generalized Hadamard Matrices, Proc. Amer. Math. Soc. 13, 894-898 (1962)
- [13] COOLEY. J.W. und TUCKEY, J.W.: An Algorithm for the Machine Calculation of Complex Fourier Series, Math. Comp. 19, 297-301 (1965)
- [14] CORBETT, J.V. und HURST, C.A.: Are wave functions uniquely determined by their position and momentum distributions, J. Austral. Math. Soc. 20 (Ser.B), 182-201 (1978)
- [15] CURTIS, C.W. und REINER, I.: Representation Theory of Finite Groups and Associative Algebras, Wiley, New York (1962)
- [16] DAVIS, Ph. J.: Circulant Matrices, Wiley, New York (1979)

- [17] DAWSON, J.E.: A construction for generalized Hadamard Matrices GH(4q,EA(q)), J. Stat. Plan. Inf. 11, 103-110 (1985)
- [18] De LAUNEY, W.: On difference matrices, transversal designs, resolvable transversal designs and large sets of mutually orthogonal F-squares, J. Stat. Plan. Inf. 16, 107-125 (1987)
- [19] ----: Square GBRDs over non-abelian groups, Ars Comb. 27, 40-49 (1989)
- [20] DENES, J. und KEEDWELL, A.D.: Latin Squares and their Applications, Academic Press, New York-London (1974)
- [21] DRAKE, D.A.: Partial λ-geometries and generalized Hadamard matrices over groups, Can. J. Math. 31, 617-627 (1979)
- [22] FEDERER, W.T. und MANDELI, J.P.: Orthog. F-rectangles, orthog. arrays, and codes, J. Comb. Theor. Ser. A 43, 149-164 (1986)
- [23] GLEASON, A.M.: Measures on the closed subspaces of a Hilbert space, J. Math. Mech. 6, 885-894 (1957)
- [24] GUDDER, S.P.: Stochastic Methods in Quantum Mechanics, North Holland, New York (1979)
- [25] ----: Quantum Probability, Academic Press, San Diego (1988)
- [26] HALMOS, P.R.: Two subspaces, Trans. Amer. Math. Soc. 144, 381-389 (1969)
- [27] HEDAYAT, A. und SEIDEN, E.: F-square and orthogonal F-squares design: A generalization of Latin square and orthogonal Latin squares design, Ann. Math. Stat. 41, 2035-2044 (1970)
- [28] HIRZEBRUCH, F. und SCHARLAU, W.: Einführung in die Funktionalanalysis, B.I., Mannheim, Wien, Zürich (1971)
- [29] HOFFMAN, K. und KUNZE, R.: Linear Algebra, 2nd. ed., Prentice-Hall, Englewood Cliffs, New Jersey (1971)
- [30] LENARD, A.: The Numerical Range of a Pair of Projections, J. Funct. Anal. 10, 410-423 (1972)
- [31] LIDL, R. und NIEDERREITER, H.: Finite Fields, Enc. of Math. and Its Appl. Vol. 20, Addison-Wesley, Reading, Mass. (1983)
- [32] LÜDERS, G.: Über die Zustandsänderung durch den Meßprozeß, Annalen der Physik 8, 322-328 (1951)
 - [33] MITTELSTAEDT, P.: Quantum Logic, Reidel, Dordrecht (1978)
 - [34] MOROZ, B.Z.: Reflections on Quantum Logic, Int. J. Theor. Phys. 22, 329-340 (1983), Erratum, Int. J. Theor. Phys. 23, 497-498 (1984)

- [35] PITOWSKY, I.: Quantum Probability Quantum Logic, Lecture Notes in Physics 321, Springer, Berlin-Heidelberg-N.Y. (1989)
- [36] RAGHAVARAO, D.: Constructions and combinatorial problems in design of experiments, corr. ed. Dover, New York (1988)
- [37] REED, M. und SIMON, B.: Methods of Modern Mathematical Physics, I: Functional Analysis, Academic Press, N.Y., 2nd.Ed. (1980)
- [38] SCHWINGER, J.: Unitary Operator Bases, Proc. Natl. Acad. Sci. U.S.A. 46, 570-579 (1960)
- [39] SEBERRY, J.: A construction for generalized Hadamard matrices, J. Stat. Plan. Inf. 4, 365-368 (1980)
- [40] SINGER, M. und STULPE, W: Informational Incompleteness of the Observables S, S, S, for Spin-1 Systems, Found. Phys. 20, 471-472 (1990)
- [41] SRINIVAS, M.D.: Foundations of Quantum Probability Theory, J. Math. Phys. 16, 1672-1685 (1975)
- [42] STULPE, W. und SINGER, M.: Some Remarks on the Determin. of Qu. States by Measurements, Found. Phys. Lett. 3, 153-166 (1990)
- [43] THIRRING, W.: Lehrbuch der Mathematischen Physik, Bd.3, Springer-Verlag, Wien-N.Y.(1979)
- [44] TURYN, R.J.: An infinite class of Williamson Matrices, J. Comb. Theor. Ser. A 12, 319-321 (1972)
- [45] VOGT, A.: Position and momentum distributions do not determine the quantum mechanical state, in: Marlow, A.R. (ed.): Mathematical Foundations of Quantum Theory, Academic Press, N.Y. (1978)
- [46] WALLIS, J.S.: Hadamard matrices, in: Wallis, W.D., Street, A.P. und Wallis, J.S.: Combinatorics: Room Squares, Sum -free Sets, Hadamard Matrices (Part IV), LNM 292, Springer, Berlin-Heidelberg-New York (1972)
- [47] WALLIS, W.D.: Combinatorial Designs, Marcel Dekker, New York and Basel (1988)
- [48] WEYL, H.: Gruppentheorie und Quantenmechanik, Leipzig (1931) Unveränd. Nachdruck der 2. Aufl. WB., Darmstadt (1981)
- [49] WIESBROCK, H.W.: Born's postulate and reconstruction of the Ψ -function in nonrelativistic quantum mechanics, Int. J. Theor. Phys. 26, 1175-1184 (1987)
- [50] WILLIAMSON, J.: Hadamard's determinant theorem and the sum of four squares, Duke Math. J. 11, 65-81 (1944)