Totientenzahlen der binären orthogonalen Geometrie

Thomas Bier

Am Badepark 16
D - 2903 Bad Zwischenahn

Germany

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3

Germany

MPI/92-76

TOTIENTENZAHLEN DER BINÄREN ORTHOGONALEN GEOMETRIE

T. Bier

Abstract

In dieser Arbeit berechnen wir die Totientenzahlen der stark regulären Graphen,deren Punktmenge aus den Elementen eines (gerade dimensionalen) Vektorraumes über dem Körper mit zwei Elementen besteht, und deren Kanten durch nicht ausgeartete quadratische Formen auf solchen Vektorräumen gegeben sind. Alternativ geben wir eine Beschreibung der Totientenzahlen als Spuren gewisser ganzzahliger symmetrischer Matrizen, die wir Hundsche Matrizen genannt haben.
Zur tatsächlichen Berechnung benötigen wir neben den inzwischen soweit bekannten Totientenzahlen arithmetischer Progressionen im n-Würfel insbesondere die Berechnung der Totientenzahlen einiger Tensorprodukte mit gewissen vierdimensionalen euklidischen Räumen, die am besten als Verallgemeinerung von Tensorprodukten mit zweidimensionalen Räumen zu verstehen sind. Diesbezüglich führen wir auch den Begriff der Stabilität bei Verdoppelungen ein.
Am Ende der Arbeit diskutieren wir noch die Frage der größtmöglichen vollständig-bipartiten Untergraphen.

1 Zwei Darstellungen von ganzzahligen Gittern in Graphen- und Matrizenräumen

Für eine Zerlegung von R^d mit ganzzahligem Untergitter Z^d in rationale Unterräume der Form

$$R^d = E_0 \perp E_1 \perp E_2 \tag{1}$$

mit $E_0 = R(1,1,...,1) = R \cdot u$ haben wir die Totientenzahlen definiert als

$$\phi(E_i) = min\{v_1 + v_2 + ... + v_d > 0 \mid (v_1, v_2, ..., v_d) \in Z^d \cap (E_0 \perp E_i)\} \quad (i = 1,2) \tag{2}$$

und haben die Produktformel $\phi(E_1) \cdot \phi(E_2) = d$ gezeigt [B1] .
In dieser Arbeit interessieren wir uns für die Berechnung dieser Zahlen im Falle einer Vektorraumzerlegung , die alternativerweise entweder durch einen bestimmten stark regulären Graphen oder auch durch ein bestimmtes Gitter in einer Matrixalgebra definiert werden kann. Zunächst betrachten wir die Definition durch den Graphen.
Sei also $V = F_2^{2h}$ ein Vektorraum über dem Körper mit zwei Elementen und betrachte eine nicht ausgeartete F_2-wertige quadratische Form Q auf V. Wir können ohne Beschränkung der Allgemeinheit annehmen, daß Q eine der beiden Gestalten

$$Q^+ = x_1x_2 + x_3x_4 + ... + x_{2h-1}x_{2h} \quad oder \quad Q^- = Q^+ + x_1^2 + x_2^2 \tag{3}$$

hat. Manchmal werden wir auch $Q = Q^+$ als diejenige quadratische Form auffassen, die durch Auswerten aller linearen Funktionen aus $W^* = Hom_{F_2}(W, F_2)$ auf dem Vektorraum $W = F_2^h$ entsteht, also

$$Q(w,\lambda) = \lambda(w) \in F_2 \quad mit \quad (w,\lambda) \in V := W \times W^* \tag{4}$$

Dann definieren wir den Graphen $V^{\pm}(2h)$ mit der Eckenmenge V und mit den Kanten $\{x,y\}$ wobei $x \neq y$ und $Q^{\pm}(x+y) = 0$ ist.
Es ist bekannt, daß die Graphen $V^{\pm}(2h)$ stark regulär sind, siehe [S1]. Insbesondere haben die $(0,1)-$charakteristischen Matrizen dieser Graphen (außer im Fall $V^-(2)$) genau drei Eigenwerte, so daß wir eine Zerlegung wie in (1) bekommen. Dabei soll die Indizierung so gewählt werden, daß im Falle der Graphen $V^{\pm}(2h)$ gilt $dim E_2 = 2^{h-1}(2^h \mp 1)$. Es ist bekannt, daß dann die Indizierung der Größe der Eigenwerte nach gewählt ist, mit den Bezeichnungen von [S1] sind also die drei Eigenwerte $k > r > s$ den Räumen E_0, E_1, E_2 zugeordnet.
Insbesondere gibt es in den quadratischen Räumen $(F_2^{2h}, Q^{\pm})$ die maximalen isotropen Unterräume der F_2-Dimension $h - \frac{1}{2} \pm \frac{1}{2}$. Im Rest dieses Abschnittes wollen wir uns auf den Fall $Q = Q^+$ beschränken. Dann sind nämlich die h-dimensionalen maximalen isotropen Unterräume von F_2^{2h} reguläre Teilmengen der Graphen $V^+(2h)$ im Sinne von [B2]. Die zugehörigen charakteristischen Vektoren dieser Mengen liegen in dem Vektorraum $E_{0,1} = E_0 \perp E_1$. Insbesondere gilt also die Teilbarkeitsbeziehung $\phi(E_1)$ teilt 2^h. Dies führt auch zu einer

Beschreibung der Vektorräume $E_{0,1}$ unabhängig von der obigen Graphentheorie. Setze nämlich

$$\mathcal{A} = \{A = a + W \mid W \ \ max\ isotroper\ UR\ von\ \ F_2^{2h}\ ,\ a \in F_2^{2h}\} \qquad (5)$$

dann ist die Definition von E_1 durch die 0, 1-charakteristischen Vektoren $c(A)$ mit $A \in \mathcal{A}$ in folgender Weise zulässig ;

$$E_{0,1} = LinSpan_R\{c(A) \mid A \in \mathcal{A}\} \qquad (6)$$

denn es gilt offenbar $E_0 \subset E_{0,1}$. Die Totientenzahlen $\phi(E_1)$ zeigen also die Existenz von Vektoren aus $E_{0,1}$ an, deren Koordinatensummen möglicherweise kleiner sind als die Koordinatensummen 2^h der charakteristischen Vektoren der maximalen isotropen Unterräume.
Hierzu wollen wir die versprochene matrizentheoretische Interpretation geben. Sei also $Mat = M_{2^h}(R)$ der Vektorraum aller reellen quadratischen $2^h \times 2^h$ Matrizen, dessen Zeilen und Spalten wir uns entweder durch $x, y \in W = F_2^h$ oder durch $\lambda, \mu \in W^*$ indiziert vorstellen. Mit $Symm$ und $Schief$ wollen wir die reellen Unterräume aller symmetrischen bzw schiefsymmetrischen Matrizen bezeichnen. Entsprechend gilt also $Mat = Symm \oplus Schief$.
Sei $R[V] = R[W \times W^*]$ der reelle Vektorraum mit Orthonormalbasis (w, λ) wie in (4) . Definiere die Abbildungen PZ, PS als

$$PZ, PS : R[V] \longrightarrow Mat \qquad (7)$$

durch die Vorschriften $PZ(w, \lambda) = N(w, \lambda)$ mit $N(w, \lambda) = (n_{xy})$ wobei

$$n_{wy} \ = \ (-1)^{\lambda(w+y)} \quad und \quad n_{xy} \ = \ 0 \quad x \neq w \qquad (8)$$

und entsprechend $PS(w, \lambda) = T(w, \lambda)$ mit $T(w, \lambda) = (t_{\xi\mu})$ wobei

$$t_{\lambda\mu} = (-1)^{(\mu+\lambda)(w)} \quad und \quad t_{\xi\mu} = 0 \quad \xi \neq \lambda \qquad (9)$$

Unmittelbar aus der Definition folgt für den Vektor $u = (1, 1, ..., 1)$ die Gleichung $PS(u) = PZ(u) = 2^h \cdot I_{2^h}$. Offenbar sind PZ und PS lineare Isomorphismen reeller Vektorräume. Es gilt

Lemma 1: $PZ(E_{0,1}) = PS(E_{0,1}) = Symm$ und $PZ(E_2) = PS(E_2) = Schief$.

Beweis : Die Eigenräume E_i haben eine Basis aus Vektoren der Form

$$u(r) = \sum_{y \in V} (-1)^{B(r,y)} \cdot y \qquad (10)$$

wobei $B(x, y) = Q(x + y) - Q(x) - Q(y)$ ist ; und zwar ist $\{u(0)\}$ eine Basis von E_0 ,

$$\{u(s) \mid Q(s) = 0, s \neq 0\}$$

ist eine Basis von E_1 und

$$\{u(a) \mid Q(a) = 1\}$$

ist eine Basis von E_2.
Andererseits haben die Matrizenräume *Symm* und *Schief* Basen aus den Heisenbergmatrizen (siehe [Q] ,[B4], [B5]) der Form

$$M(w,\lambda) = (m_{xy}) \quad mit \quad M(w,\lambda)x = (-1)^{\lambda(x)}(x+w) \tag{11}$$

Dann zeigt eine kurze Rechnung, daß für $r = (w,\lambda)$ die Beziehung

$$PZ(u(r)) = 2^h \cdot M(r)$$

gilt. □
Die Ganzzahligkeitsbedingung läßt sich dann mit Hilfe der Gitter

$$\Gamma_Z = PZ(Z[V]) \quad \Gamma_S = PS(Z[V]) \tag{12}$$

formulieren. Induktiv kann man diese Gitter auch durch das ganzzahlige Erzeugnis der vier Matrizen aus $M_2(R)$

$$\begin{matrix} 1 & 1 \\ 0 & 0 \end{matrix} \qquad \begin{matrix} 1 & -1 \\ 0 & 0 \end{matrix} \qquad \begin{matrix} 0 & 0 \\ 1 & 1 \end{matrix} \qquad \begin{matrix} 0 & 0 \\ -1 & 1 \end{matrix}$$

das wir mit $\Gamma_Z(1)$ bezeichnen wollen, und dann mit Hilfe des Isomorphismus in

$$M_2(R) \otimes M_2(R) \otimes ... \otimes M_2(R) \quad \cong \quad M_{2^k}(R)$$

als

$$\Gamma_Z(1) \otimes \Gamma_Z(1) \otimes ... \otimes \Gamma_Z(1) \quad \cong \quad \Gamma_Z$$

beschreiben. Ein entsprechender Isomorphismus gilt natürlich auch für Γ_S.
Für diese Gitter gilt dann

Lemma 2: $\Gamma_Z \cap Symm = \Gamma_S \cap Symm$
$\Gamma_Z \cap Schief = \Gamma_S \cap Schief$.

Beweis : Seien n_i gewisse Spalten der Matrizen $N(w,\lambda)$. Nun ist $A \in \Gamma_Z$ genau dann falls es ganze Zahlen a_i gibt mit $A = \sum_i a_i \cdot n_i$. Man erhält beim Transponieren der Zeilen $n_i^t = t_i$ gewisse Spalten der Matrizen $T(w,\lambda)$. Falls also $A = A^t$ symmetrisch ist, so folgt sofort $A \in \Gamma_S$. □

Da die Elemente aus $\Gamma \cap Symm$ in diesem Kontext besondere Bedeutung haben, wollen wir sagen, die Matrizen $H \in \Gamma \cap Symm$ seien *Hundsche Matrizen* . Damit können wir insbesondere die Totientenzahlen auch rein matrizentechnisch beschreiben :

Lemma 3 : Für den Raum $E_{0,1} \subset R[V^+(2h)]$ gilt mit $n = 2^h$

$\phi(E_{0,1}) = min\{h_{11} + h_{22} + ... + h_{nn} > 0 \mid H = (h_{ij}) \in \Gamma \cap Symm\}$, also ist die Totientenzahl von E_1 die kleinste positive Spur von Hundschen Matrizen.

Beweis : Zunächst beobachtet man, daß die Abbildungen PZ und PS bis auf einen skalaren Faktor von 2^h Isometrien von euklidischen Räumen mit dem kanonischen Skalarprodukt sind. Es gilt nämlich für $a, b \in V$

$$2^h \cdot < a, b >=< PZ(a), PZ(b) >$$

Sei nun H eine Hundsche Matrix , also gibt es $v \in Z[V] \cap E_{01}$ einen Vektor mit der Eigenschaft $PZ(v) = H$. Mit dem Nur-Eins-Vektor u gilt dann

$$< u, v >=< I_n, PZ(v) >= Spur(H)$$

was zu zeigen war. □

2 Eine tensorielle Hilfskonstruktion

Zunächst wollen wir eine Verdoppelungskonstruktion angeben, welche uns den Weg zur Berechnung der Totientenzahlen der obigen Graphen weisen wird. Dazu sei eine Zerlegung von R^d wie in (1) gegeben, und sei R^2 zerlegt in die Räume

$$R^2 = F_0 \perp F_1 \quad \text{mit} \quad F_0 = R(1,1) \quad \text{und} \quad F_1 = R(1,-1)$$

Dann betrachten wir die Tensorprodukte

$$R^{2d} = R^2 \otimes R^d \quad \text{und} \quad T_{ij} = F_i \otimes E_j$$

und interessieren uns insbesondere für die Zerlegung

$$R^2 \otimes R^r = T_{00} \perp (T_{01} \perp T_{12}) \perp (T_{02} \perp T_{11}) \perp T_{10}$$

deren Teilräume wir mit

$$T_1 = T_{01} \perp T_{12} \text{ und } T_2 = T_{02} \perp T_{11}$$

bezeichnen wollen. Der Sumand T_{10} wird sich dabei übrigens (falls d gerade ist) als unerheblich herausstellen.
Wir betrachten die ganzzahligen Gitter

$$\Delta_{01} = Z^d \cap (E_0 \perp E_1) \text{ und } \Delta_2 = Z^d \cap E_2$$

sowie die entsprechenden Δ_{02} und Δ_1 . Ihre Reduktionen modulo 2 seien mit

$$C_{01} = \Delta_{01}/2 \cdot \Delta_{01} \text{ sowie } C_1, C_2 \text{ usw.}$$

bezeichnet. Wir bemerken die fundamentale Tatsache, daß der F_2-Homomorphismus

$$\tau : C_{01} \longrightarrow F_2$$

der durch die Vorschrift

$$\bar{v} \longmapsto < v, u > mod 2 \quad \text{für} \quad \bar{v} \in C_{01}$$

gegeben ist , den Kern

$$Kern(\tau) = C_1$$

hat; denn offenbar ist $C_1 \subset Kern(\tau)$ und $dim_{F_2} C_1 = dim_R E_1 = dim_{F_2} Kern(\tau)$. Ausgangspunkt der folgenden Betrachtungen ist das elementare

Lemma 4 : (i) Falls $(C_{01} - C_1) \cap C_2 \neq \emptyset$ nichtleeren Durchschnitt haben, so ist

$$\phi(T_1) = \phi(E_1) \quad \text{und} \quad \phi(T_2) = \phi(T_2 \perp T_{10}) = 2 \cdot \phi(E_2)$$

(ii) Falls $C_1 \cap (C_{02} - C_2) \neq \emptyset$ nichtleeren Durchschnitt haben, so ist

$$\phi(T_1) = \phi(T_1 \perp T_{10}) = 2 \cdot \phi(E_1) \quad \text{und} \quad \phi(T_2) = \phi(E_2)$$

Beweis: Offenbar genügt es, einen Teil, etwa (i) zu zeigen. Dazu beobachten wir zuerst, daß die Elemente in $C_{01} - C_1$ durch solche ganzzahligen Vektoren v dargestellt werden, die in $v \in \Delta_{01}$ liegen und welche die Gleichung

$$< v, u >= (2s + 1) \cdot \phi(E_1)$$

für irgendeine ungerade Zahl $2s + 1$ erfüllen. Sei nun die mod 2 Reduktion $\bar{v}$ in $\bar{v} \in (C_{01} - C_1) \cap C_2$ gelegen, dann gibt es einen ganzzahligen Vektor $w \in \Delta_2$ mit $\bar{v} = \bar{w}$. Nun hat der Vektor

$$(1,1) \otimes v \; + \; (1,-1) \otimes w \quad \in \quad T_{00} \perp T_{01} \perp T_{12}$$

nur gerade ganzzahlige Koordinaten, und somit ist der Vektor

$$x = \frac{1}{2}((1,1) \otimes v \; + \; (1,-1) \otimes w) \in \; T_{00} \perp T_{01} \perp T_{12}$$

ganzzahlig und zeigt wegen

$$< x, (1,1) \otimes u >=< v, u >= (2s + 1) \cdot \phi(E_1)$$

sowie wegen der Existenz eines Vektors y aus $y \in \Delta_{01}$ mit $< y, u >= \phi(E_1)$, woraus doch

$$< (1,1) \otimes y, (1,1) \otimes u >= 2 \cdot \phi(E_1)$$

folgt, die Teilbarkeitsbeziehung

$$\phi(T_{01} \perp T_{12}) \quad \text{teilt} \quad \phi(E_1)$$

Mit demselben Argument, aber leichter zu zeigen, ist

$$\phi(T_{02} \perp T_{11}) \quad \text{teilt} \quad 2 \cdot \phi(E_2)$$

und aus der Produktformel für die Totientenzahlen folgt Gleichheit :

$$\phi(T_1) = \phi(E_1) \quad \text{und} \quad \phi(T_2) = 2 \cdot \phi(E_2)$$

Das war zu zeigen. □
Wir merken an, daß insbesondere höchstens einer der beiden folgenden Durchschnitte nichtleer sein kann:

$$(C_{01} - C_1) \cap C_2 \quad \text{oder} \quad C_1 \cap (C_{02} - C_2)$$

Zunächst betrachten wir den Fall d ungerade. Dann sind für irgendeine Zerlegung der Form

$$R^2 \otimes R^d = T_0 \perp G_1 \perp G_2$$

mit $T_{10} \perp T_{01} \subset G_1$ und $T_{02} \subset G_2$ die Totientenzahlen durch

$$\phi(G_1) = \phi(E_1) \quad \text{und} \quad \phi(G_2) = 2 \cdot \phi(E_2)$$

gegeben; denn in G_1 liegen die ganzzahligen Vektoren

$$\frac{1}{2}[(1,1) \otimes u + (1,-1) \otimes u] \quad \in \quad T_{00} \perp T_{10}$$

welcher $\phi(G_1)$ teilt d zeigt und für $v \in E_0 \perp E_1$ mit $< v, u >= \phi(E_1)$

$$(1,1) \otimes v \quad \in \quad T_{00} \perp T_{01}$$

welcher $\phi(G_1)$ teilt $2 \cdot \phi(E_2)$ zeigt, zusammen also folgt wegen d ungerade : $\phi(G_1)$ teilt $\phi(E_1)$. Genauso aber leichter gilt $\phi(G_2)$ teilt $2 \cdot \phi(E_2)$.
Entsprechend behandelt man den Fall einer Zerlegung

$$R^2 \otimes R^d = T_0 \perp H_1 \perp H_2$$

mit $T_{01} \subset H_1$ und $T_{10} \perp T_{02} \subset H_2$, wo gilt

$$\phi(H_1) = 2 \cdot \phi(E_1) \quad \text{und} \quad \phi(H_2) = \phi(E_2)$$

In dem Fall d ungerade ist also keine der beiden Voraussetzungen des Lemma 4 erfüllt ; jeder der beiden Durchschnitte

$$(C_{01} - C_1) \cap C_{02} = \emptyset \quad \text{und} \quad C_{01} \cap (C_{02} - C_2) = \emptyset$$

muß leer sein; anderenfalls erhielte man durch Verschieben von T_{10} auf eine der beiden Seiten einer Zerlegung aus Lemma 4 einen Widerspruch zu den gerade berechneten Totientenzahlen.
Im Fall d gerade gilt hingegen :

Folgerung : Für d gerade ist genau einer der beiden Durchschnitte

$$(C_{01} - C_1) \cap C_2 \quad \text{oder} \quad C_1 \cap (C_{02} - C_2) \tag{13}$$

nichtleer.

Um das zu zeigen, genügt es, die Annahme

$$(C_{01} - C_1) \cap C_2 = \emptyset \quad \text{und} \quad C_1 \cap (C_{02} - C_2) = \emptyset \tag{14}$$

zum Widerspruch zu führen. Wegen einer offensichtlichen Teilbarkeitsbeziehung, die genau wie im Fall d ungerade gezeigt werden kann, sehen wir zunächst, daß genau eine der beiden Alternativen (15) oder (16) gelten muß:

$$\phi(T_{10} \perp T_{01} \perp T_{12}) = \phi(E_1) \ \text{ und } \ \phi(T_{02} \perp T_{11}) = 2 \cdot \phi(E_2) \tag{15}$$

$$\phi(T_{10} \perp T_{01} \perp T_{12}) = 2 \cdot \phi(E_1) \ \text{ und } \ \phi(T_{02} \perp T_{11}) = \phi(E_2) \tag{16}$$

Im Fall (15) gibt es einen ganzzahligen Vektor $x \in T_{00} \perp T_{10} \perp T_{01} \perp T_{12}$, der die Gleichung $< x, (1,1) \otimes u >= \phi(E_1)$ erfüllt. Diesen Vektor x spalten wir dann auf als

$$x = (1,1) \otimes v \ + \ (1,-1) \otimes w \quad \text{mit} \ \ v \in E_0 \perp E_1 \ \ \ w \in E_0 \perp E_2 \ .$$

so daß wegen der Ganzzahligkeit von x auch die Vektoren $v \pm w$ ganzzahlig sind. Also sind auch $V = 2v$ und $W = 2w$ ganzzahlig und es gilt $V_i \equiv W_i \ mod\ 2 \ \ \forall\, i = 1, ..., d$. Weiterhin ist

$$< V, u >= 2 \cdot < v, u >=< x, (1,1) \otimes u >= \phi(E_1)$$

und somit liegt $\bar{V} = \bar{W} \in (C_{01} - C_1) \cap C_{02}$. Nach der ersten Gleichung der Annahme (14) ist also $\bar{W} \in (C_{02} - C_2)$ und also ist

$$< W, u >= (2s + 1) \cdot \phi(E_2)$$

Somit ist einerseits durch Projektion auf die von u aufgespannte Gerade

$$< V, W >=< \frac{< V, u >}{< u, u >} \cdot u, \frac{< W, u >}{< u, u >} \cdot u >= \frac{< V, u > \cdot < W, u >}{< u, u >} \equiv 1 \ \ mod\ 2$$

andererseits aber ist wegen unser Voraussetzung $d \equiv 0 \ \ mod\ 2$ auch entweder $< V, u >= \phi(E_1)$ oder $< W, u >= \phi(E_2)$ gerade, und wegen $V_i \equiv W_i \ \ mod\ 2$ folgt der Widerspruch

$$1 \equiv \sum_{i=1}^{d} V_i \cdot W_i \equiv \sum_{i=1}^{d} V_i^2 \equiv \sum_{i=1}^{d} V_i \equiv 0 \quad mod\ 2$$

oder genauso mit W_i statt V_i. Damit ist die Alternative (15) zum Widerspruch geführt.

Falls hingegen (16) gelten sollte, argumentieren wir ganz ähnlich: Nach Annahme muß es ein $y \in T_{00} \perp T_{02} \perp T_{11}$ geben mit $< y,(1,1) \otimes u >= \phi(E_2)$. Wir spalten dann auf

$$y = (1,1) \otimes v \; + \; (1,-1) \otimes w \;\; \text{mit} \;\; v \in E_0 \perp E_2 \;\; w \in E_1$$

Es gilt $v \pm w \in Z^d$, also sind $V = 2v$ und $W = 2w$ beide ganzzahlig mit $\bar{V} = \bar{W}$ und wegen

$$< V, u >= 2 \cdot < v, u >=< y,(1,1) \otimes u >= \phi(E_2)$$

ist $V \in (C_{02} - C_2)$. Wegen $\bar{V} = \bar{W} \in C_1$ folgt ein Widerspruch zur zweiten Gleichung der Annahme (14). Somit ist die Folgerung (13) gezeigt. □
Falls also für d gerade der Durchschnitt $(C_{01} - C_1) \cap C_2 \neq \emptyset$ nichtleer ist, wollen wir sagen, der Raum E_1 sei ***stabil bei Verdoppelung*** . Entsprechend genauso für E_2 . Somit gilt: Für d gerade ist genau einer der beiden Räume E_1 , E_2 stabil bei Verdoppelung.

Wir nehmen nun an, es sei eine Zerlegung von R^d wie in (1) gegeben, und außerdem sei R^4 in der folgenden Weise zerlegt :

$$R^4 = G_0 \perp G_1 \perp G_2$$

mit den Räumen

$$G_0 = R(1,1,1,1) \;\; G_1 = R(1,1,-1,-1) \perp R(1,-1,-1,1) \;\; G_2 = R(1,-1,1,-1)$$

Wir wollen die Tensorprodukte

$$T = R^4 \otimes R^d \qquad T_{ij} = G_i \otimes E_j$$

und dabei insbesondere die Zerlegung

$$R^{4d} = T = T_{00} \perp (\, T_{01} \perp T_{10} \perp T_{11} \perp T_{22} \,) \perp (\, T_{02} \perp T_{20} \perp T_{21} \perp T_{12}) \quad (17)$$

betrachten. Zur Abkürzung wollen wir noch

$$T_0 = T_{00}$$

$$T_1 = T_{10} \perp T_{01} \perp T_{11} \perp T_{22}$$

$$T_2 = T_{20} \perp T_{02} \perp T_{12} \perp T_{21}$$

setzen. Dann gilt
Lemma 5: Sei in der Zerlegung (1) $\phi(E_1) \equiv 0 \; mod \; 2$ und es seien drei Vektoren in R^d mit ganzen Komponenten wie folgt gegeben :

$$v \in E_{02} \;\; mit \;\; < v, u >= 2 \cdot \phi(E_2)$$

$$w \in E_{01} \quad mit \quad w_i \equiv v_i \ mod\ 4 \quad \forall i = 1, ..., d$$

$$x \in E_2 \quad mit \quad x_i \equiv w_i \ mod\ 2 \quad \forall i = 1, ..., d$$

Dann gilt für die Totientenzahlen der Zerlegung (13) die Abschätzung

$$\phi(T_2) \quad \text{teilt} \quad 2 \cdot \phi(E_2) \tag{18}$$

Beweis: Wir setzen zunächst

$$m = \frac{d}{2\phi(E_2)}$$

was nach Voraussetzung ganz ist. Weiterhin betrachten wir den ganzzahligen Vektor

$$y = m \cdot v - u$$

für dessen Komponenten y_i nach Voraussetzung gilt

$$y_i \equiv k \cdot m - 1 \ mod\ 4m \quad \Leftrightarrow \quad v_i \equiv k \ mod\ 4 \quad \Leftrightarrow \quad w_i \cdot m \equiv k \cdot m \ mod\ 4m$$

Somit folgen für die Komponenten der Vektoren $y \pm m \cdot w$ die Kongruenzen

$$y_i - m \cdot w_i \equiv \quad -1 \ mod\ 4m$$

$$y_i + m \cdot w_i \equiv \quad -1 \ mod\ 4m \quad \Leftrightarrow \quad w_i \equiv 0 \ mod\ 2$$

$$y_i + m \cdot w_i \equiv \ 2m - 1 \ mod\ 4m \quad \Leftrightarrow \quad w_i \equiv \ 1 \ mod\ 2$$

Infolgedessen erfüllt der Vektor

$$t \ = \ (1,1,1,1) \otimes y + m \cdot (1,-1,1,-1) \otimes w + 2m \cdot (1,0,-1,0) \otimes x \tag{19}$$

aus $t \in T_2$ in allen Komponenten die Kongruenz

$$t_k \equiv \ -1 \ mod\ 4m \quad \forall \ \ k = 1, ..., 4d$$

und somit hat

$$\frac{1}{4m}(t + (1,1,1,1) \otimes u) \quad \text{aus} \ \ T_0 \perp T_2$$

ganze Komponenten. □

Um dies anwenden zu können, benötigen wir noch den Bezug zur obigen Graphentheorie. Wir setzen dazu die Eigenraumzerlegungen der entsprechenden stark regulären Graphen an als

$$R[V^+(2)] = G_0 \perp G_1 \perp G_2$$

$$R[V^+(2h)] = E_0 \perp E_1 \perp E_2$$

Dann ist die gesuchte Beziehung recht offensichtlich:
Lemma 6 : Unter der Zerlegung

$$V^+(2h+2) = V^+(2) \perp V^+(2h)$$

bezüglich der bilinearen Form $B(x,y) = Q(x+y) + Q(x) + Q(y)$ über dem Körper F_2 gilt für das Tensorprodukt

$$R[V^+(2h+2)] = R[V^+(2)] \otimes R[V^+(2h)] \quad : \tag{20}$$

Die Zerlegung

$$R[V^+(2h+2)] = T_0 \perp T_1 \perp T_2$$

aus Gleichung (17) ist genau die Zerlegung in die Eigenräume des Graphen $V^+(2h+2)$.

Der Beweis ist eine rein formale Zerlegung der $(0,1)$-Matrizen und soll hier nicht ausgeführt werden.
Schließlich benötigen wir noch eine spezielle Eigenschaft von Eigenvektoren bei der Tensorzerlegung. Sei dazu wieder bezüglich der Bilinearform $B(x,y) = Q(x+y) + Q(x) + Q(y)$ die orthogonale Zerlegung

$$V^-(2h+2) = V^-(2h) \perp V^+(2) \ ,$$

die zugehörige Tensorzerlegung

$$R[V^-(2h+2)] = R[V^-(2h)] \otimes R[V^+(2)]$$

und die Zerlegung in die Eigenräume der $(0,1)$-Matrizen

$$R[V^-(2h+2)] = T_0 \perp T_1 \perp T_2$$

gegeben. Wir wollen die Punkte $x \in V^-(2h+2)$ schreiben als $x = (a,b)$ mit $a \in V^-(2h)$ und $b \in V^+(2) = \{0,e,f,g\}$ $(Q(g) = 1)$.

Lemma 7: Für einen Vektor $z \in T_0 \perp T_2$ ist der Vektor $\tilde{x}$ mit den Komponenten

$$\tilde{x}_a = z_{a0} - z_{ae} - z_{af} + z_{ag}$$

ein Eigenvektor mit

$$\tilde{x} \in E_2 \subset R[V^-(2h)]$$

Der Beweis ist ein einfaches formales Argument und wird hier nicht ausgeführt.

3 Die Totientenzahlen der orthogonalen Geometrie modulo 2

Jetzt können wir das Hauptergebnis dieser Arbeit formulieren und beweisen. Dazu setzen wir $\phi_i(V^{\pm}(2h)) = \phi(E_i)$ mit $E_i \subset R[V^{\pm}(2h)]$ wie nach Gleichung

(4) festgelegt.

Satz : (i) Für $h = 2m$ gilt

$$\phi_1(V^{\pm}(4m)) = 2^{m+1} \qquad \phi_2(V^{\pm}(4m) = 2^{3m-1}$$

(ii) Für $h = 2m + 1$ (aber $m > 0$ im Falle $V^+(2)$!) gilt

$$\phi_1(V^{\pm}(4m+2)) = 2^{m+2} \qquad \phi_2(V^{\pm}(4m+2)) = 2^{3m}$$

(iii) Für $h = 1$ gilt

$$\phi_1(V^+(2)) = \phi_2(V^+(2)) = 2$$

Insbesondere existieren also für $h > 3$ stets ganzzahlige Vektoren aus $E_{0,1} \subset R[V^+(2h)]$ deren Koordinatensummen kleiner sind als 2^h.

Beweis : Für die meisten Fälle reicht das Ergebnis aus [B3] aus. Wir benutzen eine bijektive Abbildung vom hyperkubischen Assoziationsschema $H(h, 4)$ nach $V^e(2h)$ mit $e = (-1)^h$ die wie folgt definiert ist. Zunächst wählen wir als zugrundeliegendes Alphabet F mit $|F| = 4$ und $H(h, 4) = F^h$ die Menge $F = V^-(2)$. Dann setzen wir

$$f : H(h, 4) \longrightarrow V^e(2h) \quad e = (-1)^h \tag{21}$$

an als $f(a_1, a_2, ..., a_h) = a_1 + a_2 + ... + a_h$ wobei die Summe im F_2-Vektorraum F_2^{2h} zu nehmen ist. Offenbar ist f eine bijektive Abbildung . Nun ist die quadratische Form auf V durch eine orthogonale direkte Summenzerlegung in h Summanden der Form $V^-(2)$ gegeben. Das ist äquivalent zur folgenden Gleichung mit dem Hamminggewicht wt_H von $H(h, 4)$:

$$Q(f(a_1, a_2, ..., a_h)) = 1 \Leftrightarrow wt_H(a_1, a_2, ..., a_h) \equiv 1(2) \tag{22}$$

Daraus folgt sofort eine Entsprechung der Eigenräume von $H(h, 4)$, die wir als

$$R[H(h, 4)] = F_0 \perp F_1 \perp ... \perp F_h \tag{23}$$

bezeichnen wollen, mit den Räumen E_i ; nämlich es gilt

$$E_2 = F_1 \perp F_3 \perp F_5 \perp .... \tag{24}$$

$$E_1 = F_2 \perp F_4 \perp F_6 \perp .... \tag{25}$$

Nun können wir das Ergebnis aus [B3] verwenden, wonach die Totientenzahlen gerade die angegebenen Werte haben. Das beendet den Beweis von (i) im Falle plus und den Beweis von (ii) im Falle minus .
Der Beweis von (i) im Falle minus kann nun sehr leicht gefolgert werden. Zunächst zerlegt man als quadratische Räume über dem Körper F_2 $V^-(4m) = V^-(4m - 2) \perp V^+(2)$ wobei die Orthogonalität bezüglich der bilinearen Form $B(x, y) = Q(x + y) - Q(x) - Q(y)$ zu verstehen ist. Dann ist dadurch auch eine Zerlegung

der Eigenräume E_i des größeren durch vier des kleineren Graphen induziert. Insbesondere ist leicht zu sehen, daß für einen Vektor $v \in E_{0,2} \subset R[V^-(4m-2)]$ der Vektor $(v,v,v,v) \in E_{0,2} \subset R[V^-(4m)]$ somit zu $\phi_2(V^-(4m))$ teilt 2^{3m-1} führt.
Andererseits betrachten wir die Orthogonalprojektion $P_{0,1}$ eines Basisvektors $x = (w,\lambda) \in R[V]$ in den Unterraum $E_{0,1}$. Dieser Vektor $P_{0,1}(x)$ kann bis auf ein skalares Vielfaches c nach [S] dargestellt werden als

$$c \cdot P_{0,1}(x) = (2^{2m}-1) \cdot x - \sum_{y \neq x} (-1)^{Q(x+y)} \cdot y$$

Daraus ergibt sich die folgende Rechnung für Teilräume $V^+(2m) \perp V^-(2m) = V^-(4m)$

$$c \cdot \sum_{x \in V^+(2m)} (-1)^{Q(x)} P_{0,1}(x) =$$

$$\sum_{x \in V^+(2m)} \{(-1)^{Q(x)}(2^{2m}-1)x + \sum_{y \in V^-(4m)-\{x\}} (-1)^{Q(x)+Q(x+y)+1} y\} =$$

$$2^{2m} \cdot \sum_{x \in V^+(2m)-\{0\}} (-1)^{Q(x)} x - 2^{2m} \cdot \sum_{y \in V^-(2m)-\{0\}} (-1)^{Q(y)} e_y$$

woraus sofort folgt, daß der Vektor

$$v = \sum_{x \in V^-(2m)-\{0\}} (-1)^{Q(x)} x - \sum_{y \in V^-(2m)-\{0\}} (-1)^{Q(y)} y$$

sich in $v \in E_{0,1} \cap Z[V^-(4m)]$ befindet. Also folgt

$$\phi_1(V^-(4m)) \ \ teilt \ \ < v,u >= 2^{m+1}$$

und somit ist (i) auch im Falle minus gezeigt.
In dem noch verbleibenden (ii) Fall plus sieht man mit einem ganz ähnlichen Argument, daß für die Zerlegung $V^+(2m) \perp V^+(2m+2) = V^+(4m+2)$ der Vektor

$$v = 3 \cdot (0) + \ 2 \cdot \sum_{x \in V^+(2m)-\{0\}} (-1)^{Q(x)} x + \sum_{x \in V^+(2m+2)-\{0\}} (-1)^{Q(x)} x$$

(wobei (0) den Nullvektor aus $V^+(4m+2)$ bezeichnet) in
$v \in E_{0,1} \cap Z[V^+(4m+2)]$ liegt. Somit gilt

$$\phi_1(V^+(4m+2)) \ \ teilt \ \ < v,u >= 2^{m+2}$$

was den ersten Teil von (ii) Fall plus zeigt.
Den zweiten Teil von (ii) Fall plus erhält man durch eine Verschärfung der Methode aus [B3], die etwas mehr Mühe erfordert. Dazu übernehmen wir die

Notationen von [B3], Seite 91 . Zunächst verifizieren wir die folgende Gleichung für ganze Zahlen k mit $0 < k < 2m$:

$$\sum_{j=0}^{m-1} \frac{f_m(1-2j)}{g_m} \binom{2m-k}{2j+1-k} = (-1)^{m-1} \cdot 2^{2m-a(m)-k} \cdot \frac{2m-k}{m} \cdot \binom{k-1}{k-m} \qquad (26)$$

Beweis: Die Formel ist trivial für kleine Werte von m. Wir nehmen daher an, sie sei für m und alle k schon bewiesen ; und sie sei auch bei gegebenem $m+1$ für gewisse Werte von k , etwa für $k > l$ schon bewiesen. Dann wollen wir sie für $k = l$ zeigen. Damit das legitim ist, müssen wir zunächst bei gegebenem $m+1$ den Induktionsanfang , also die Gleichung für $k = 2m+1$ beweisen. In diesem Falle jedoch besteht die Summe nur aus einem einzigen Term, nämlich $\frac{f_{m+1}(1-2m)}{g_{m+1}} \cdot \binom{1}{0}$. Diese ganze Zahl ist offenbar gleich der ganzen Zahl $(-1)^m \cdot 2^{1-a(m+1)} \cdot \frac{1}{m+1} \cdot \binom{2m}{m}$ wie man durch Betrachtung des Vorzeichens und der verschiedenen darin aufgehenden Primzahlpotenzen feststellen kann.
Im Weiteren werden wir den Ausdruck

$$c_j(m) := \frac{f_m(1-2j)}{g_m} \qquad (27)$$

als Abkürzung verwenden. Aus Gleichung (1) von [B3] entnehmen wir für ganze Zahlen a die folgende Gleichung

$$-\frac{1}{g_{m+1}} \cdot \Delta^{2m+2-l} f_{m+1}(a) = -\frac{2}{g_{m+1}} \cdot \Delta^{2m+1-l} f_{m+1}(a+1) + \frac{2^{\nu_2(m+1)+1}}{g_m} \cdot \Delta^{2m-l} f_m(a+2) \qquad (28)$$

Für den Wert $a = -2m-2$ bekommen wir durch Weglassen je eines Summanden vor und hinter dem Gleichheitszeichen

$$\sum_{j=0}^{m} c_j(m+1) \cdot \binom{2m+2-l}{2j+1-l} = 2^{\nu_2(m+1)+1} \cdot \sum_{j=0}^{m} c_j(m) \binom{2m-l}{2j+1-l} + 2 \cdot \sum_{j=0}^{m} c_j(m+1) \binom{2m+2-(l+1)}{2j+1-(l+1)} \qquad (29)$$

In diesen Ausdruck setzen wir die Induktionsvoraussetzung zweimal in die rechte Seite ein. Nach einer gewissen Vereinfachung, die wir hier unterdrücken wollen, erhalten wir dann als Ergebnis in Gleichung (29)

$$(-1)^m \cdot 2^{2m+2-a(m+1)-l} \cdot \frac{2m+2-l}{m+1} \cdot \binom{l-1}{l-m-1}$$

was genau dem Wert für Gleichung (26) mit $m+1$ statt m und mit l statt k entspricht. Damit ist Gleichung (26) bewiesen. □
Die Gleichung (26) gilt auch noch für $k = 0$, falls wir (nur für diesen speziellen Fall) die Übereinkunft $\binom{-1}{-m} = (-1)^m$ treffen .
Nun sei $0 \in R[H(2m,4)]$ der Basisvektor, der dem Nullpunkt entspricht, und

betrachte (bis auf einen konstanten Faktor, den wir im folgenden stets unterdrücken werden) die Projektion dieses Vektors $P_j(0)$ in den Eigenraum F_j . Wir werden jetzt die Koordinaten des Vektors

$$\sum_{i=0}^{m-1} c_i(m) \cdot P_{2i+1}(0) - 2^{2m-\alpha(m)} \cdot u \tag{30}$$

berechnen. Aus [B6] entnehmen wir die Formel für die Krawtchouk-Polynome, welche den Wert eines Vektors $P_j(0)$ an der Stelle x mit $wt(x) = d$ angibt. Insgesamt erhalten wir als die Komponente von (30) an einer solchen Stelle

$$\sum_{i=0}^{m-1} \sum_{k=0}^{2i+1} (-1)^k c_i(m) \cdot \binom{2m-k}{2i+1-k} \binom{2m-d}{k} \cdot q^k \tag{31}$$

was sich nach einer kleinen Zwischenrechnung mit Hilfe von Formel (26) zu

$$\sum_{k=0}^{2m-1} (-1)^{k+m} \cdot 2^{2m-\alpha(m)-k} \cdot \frac{2m-k}{m} \cdot \binom{k-1}{k-m} \cdot \binom{2m-d}{k} q^k \tag{32}$$

vereinfacht. Diesem Ergebnis entnehmen wir dann offenbar, daß für $k < m$ der Koeffizient von q^k Null ist, unabhängig von d .Ab jetzt wollen wir q als gerade ganze Zahl voraussetzen. Dann ist die ganze Zahl in (32) außerdem immer durch

$$2^{m-\alpha(m)} \cdot q^m$$

teilbar. Nach dem Herausteilen ergibt sich ein Vektor

$$V = \frac{1}{2^{m-\alpha(m)} \cdot q^m} \cdot \sum_{i=0}^{m-1} c_i(m) \cdot P_{2i+1}(0) - \quad 2^m \cdot u$$

in $F_0 \perp F_1 \perp \ldots \perp F_{2m-1}$ und als dessen Komponenten Polynome in q , deren konstante und lineare Terme sich als

$$\binom{2m-d}{m} - (m-1)\binom{2m-d}{m+1} \cdot \frac{q}{2} \tag{33}$$

ergeben, und deren weitere Terme alle die Faktoren

$$\frac{q^s}{2^s}$$

mit $s > 1$ in sich tragen. Falls nun speziell $q = 4$ gesetzt wird, was im Folgenden allein interessiert, so können wir schließen, daß für alle $x \in H(2m, 4)$ mit $wt(x) = d$ der in Betrachtung stehende Wert der Komponente des Vektors V an der Stelle x der Kongruenz

$$V_x \equiv (-1)^{m-d} \cdot \binom{2m-d}{m} \mod 4 \tag{34}$$

genügt, was nur für $m-d$ ungerade überhaupt etwas Neues aussagt; und was sich aus (33) durch die Fallunterscheidung m gerade und m ungerade auch leicht zeigen läßt.
Ganz ähnlich wie oben und sogar etwas leichter läßt sich für ganze Zahlen k mit $0 \leq k \leq 2m$ auch die Gleichung

$$\sum_{i=0}^{m} c_i(m) \cdot \binom{2m-k}{2i-k} = (-1)^m \cdot \binom{k}{k-m} \cdot 2^{2m-a(m)-k} \tag{35}$$

beweisen. Daraus kann man dann ganz genau wie oben die Koordinaten des Vektors

$$\sum_{i=0}^{m} c_i(m) \cdot P_{2i}(0)$$

bestimmen und erhält für diese an der Stelle $x \in H(2m,4)$ mit $wt(x) = d$ den Wert

$$\sum_{k=0}^{2m} (-1)^{k+m} \cdot 2^{2m-a(m)-k} \binom{k}{k-m} \binom{2m-d}{k} q^k \tag{36}$$

ein Wert, welcher für $k < m$ offenbar immer Null sein muß, und welcher für $d = m$ sich als

$$2^{m-a(m)} \cdot q^m$$

ergibt. Also sind für gerades q die Werte der Komponenten für beliebiges d alle durch $2^{m-a(m)} \cdot q^m$ teilbar. Im Spezialfall $q = 4$ erhält man durch eine binomiale Identität als die Werte der Quotienten gerade

$$(-1)^{m-d} \cdot \binom{2m-d}{m} \tag{37}$$

Wir haben also einen ganzzahligen Vektor in $F_0 \perp F_2 \perp \ldots \perp F_{2m}$ gefunden, nämlich

$$W = \frac{1}{2^{3m-a(m)}} \sum_{i=0}^{m} c_i(m) \cdot P_{2i}(0)$$

Aus Gleichungen (34) und (37) folgt dann für alle $x \in H(2m,4)$ die Kongruenz

$$V_x \equiv W_x \mod 4 \tag{38}$$

Ganz ähnlich wie oben betrachten wir nun den Vektor Z in $R[H(2m+1,4)]$

$$2^{3m+1} \cdot Z = \sum_{i=0}^{m} c_i(m) \cdot P_{2i+1}(0) - 2^{2m-a(m)} \cdot u \in F_0 \perp F_1 \perp F_3 \perp \ldots \perp F_{2m+1} \tag{39}$$

Nach dem Ausdividieren des gemeinsamen Faktors von 2^{3m+1} erhalten wir einen Vektor , dessen Komponente an der Stelle $x \in H(2m+1,4)$ mit $wt(x) = d$ durch die Formel

$$Z_x = z_d = \sum_{j=0}^{m-d} (-1)^j \cdot \binom{m+j}{j} \tag{40}$$

gegeben ist. Insbesondere ist also Z_x ganz und $Z_x = 0$ für $d > m$. Wir können Z auch auffassen als einen Vektor in $E_0 \perp E_2 \subset R[V^-(4m+2)]$. Bei einer Zerlegung wie in Lemma 7 definieren wir ganze Zahlen

$$\tilde{X}_a = Z_{a0} - Z_{ae} - Z_{af} + Z_{ag} \tag{41}$$

und erhalten somit einen Vektor

$$\tilde{X} \in E_2 \subset R[V^-(4m)] \tag{42}$$

Zum Schluß zerlegen wir noch einmal

$$V^-(4m) = V^-(4m-2) \perp V^+(2) \tag{43}$$

und führen bezüglich der Partition $V^-(4m) = A \cup B$

$$A = V^-(4m-2) \cup V^-(4m-2)+g$$

$$B = V^-(4m-2)+e \cup V^-(4m-2)+f$$

einen Seidel-Switching-Prozess durch [S2], insbesondere Abschnitt 3 und Abschnitt 9 ; und erhalten auf diese Weise einen Graphen der Form $V^+(4m)$. Unter dem Seidel-Switching-Prozess entsprechen sich die Räume $E_2 \subset R[V^-(2h)]$ und $E_0 \perp E_1 \subset R[V^+(4m)]$. Wir erhalten also aus dem Vektor $\tilde{X} \in E_2 \subset R[V^-(4m)]$ einen Vektor $X \in E_0 \perp E_1$ in dem Raum $R[V^+(4m)]$. Es ist leicht zu sehen, daß der Seidel-Switching-Prozess bei einem Vektor die eine 'Hälfte' der Koordinaten, etwa diejenigen aus B, mit einem Minuszeichen versieht, und die anderen, etwa diejenigen aus A unverändert läßt. Wenn wir den beschriebenen Prozess sorgfältig verfolgen und am Anfang die Koordinaten von Z einsetzen, sehen wir, daß der Vektor X an der Stelle

$$a = (y,b) \in V^-(4m) = V^-(4m-2) \perp V^+(2) \quad \text{und} \quad d = wt(y)$$

die Koordinaten

$$X_{y0} = \pm(z_d + z_{d+1} - 2z_{d+2})$$

$$X_{ye} = X_{yf} = X_{yg} = \pm(z_{d+1} - z_{d+2})$$

hat. Offenbar gilt nun

$$\pm(z_d \pm z_{d+1}) \equiv \binom{2m-d}{m} \mod 2 \tag{44}$$

und somit erhält man endlich bei entsprechender Berücksichtigung der Gewichte $wt(x)$ in $H(2m,4)$ auch die Kongruenz

$$W_x \equiv X_x \mod 2 \quad \forall \; x \in V^+(4m) \tag{45}$$

Damit sind die Voraussetzungen von Lemma 5 erfüllt. Aus Lemma 5 und 6 folgt dann die gewünschte Teilbarkeitsbeziehung für (ii) im Fall plus. □

Wir wollen noch bemerken, daß die Konstruktion in diesem letzten Fall , also die Abschätzung für $\phi_2(V^+(4m+2))$ deshalb so kompliziert war, weil die konstruierten Vektoren $X \in R[H(2m,4)]$ **nicht** die Eigenschaft (nach [D] auch *Kronen um Null* genannt)

$$wt(x) = wt(y) \Longrightarrow X_x = X_y$$

hatten. Natürlich sind auch die Vektoren, welche für die Abschätzung von $\phi_1(V^{\pm}(2h))$ benützt wurden, keine Kronen um Null. Die Tatsache, daß man für die meisten (aber eben wohl doch nicht für alle) Abschätzungen $\phi_2(V^{\pm}(2h))$ mit Kronen um Null auskommt, ist wohl eher zufällig. Eine wichtigere Rolle scheinen gewisse Symmetrieeigenschaften der Vektoren zu spielen.

4 Codes als Reduktion ganzzahliger primitiver Untergitter

Für das Gitter $Z^d \subset R^d$ und einen euklidischen Unterraum $E_i \subset R^d$ heißt bekanntlich das Gitter $\Delta_i = Z^d \cap E_i$ in E_i ein *primitives Untergitter* von Z^d. Wir wollen nun, motiviert durch die Betrachtungen im zweiten Abschnitt, für eine gegebene Zerlegung $R^d = E_0 \perp E_1 \perp E_2$ (mit E_0 beliebig) und eine Primzahl p das Schnittverhalten der (linearen) Codes

$$C_i = \Delta_i / p \cdot \Delta_i$$

$$C_{ij} = \Delta_{ij} / p \cdot \Delta_{ij}$$

mit $\Delta_{ij} = Z^d \cap (E_i \perp E_j)$ studieren. Dazu dient zunächst einmal die folgende triviale Bemerkung

$$p \text{ teilt } det(\Delta_0) \iff C_0 \cap C_{12} \neq \emptyset \tag{46}$$

Das ist sehr leicht zu sehen, denn in der Tat gibt es eine injektive lineare Abbildung von F_p-Vektorräumen

$$i_p : C_0 \cap C_{12} \rightarrow Z^d / \Delta_0 \perp \Delta_{12}$$

mit der Eigenschaft

$$Bild(i_p) = \{a \in Z^d / \Delta_0 \perp \Delta_{12} \mid p \cdot a = 0\}$$

Genauer ist also der p-Rang der Gruppe $Z^d / \Delta_0 \perp \Delta_{12}$ gleich der F_p-Dimension von $C_0 \cap C_{12}$.
Daraus können wir nun leicht einen Schluß ziehen, der das Schnittverhalten im Sinne von Abschnitt 2 bestimmt :
Falls p nicht $det(\Delta_0)$ teilt, so gilt

$$(C_{01} - C_1) \cap C_2 = \emptyset \quad \text{und} \quad C_1 \cap (C_{02} - C_2) = \emptyset \tag{47}$$

Falls nämlich $(C_{01} - C_1) \cap C_2 \neq \emptyset$ wäre, so gäbe es $c_2 = c_0 + c_1$ mit $c_0 \neq 0$ in $C_0 \subset C_{01}$ und somit käme der Widerspruch $0 \neq c_0 = c_2 - c_1$ zu Gleichung (46) . Die Gleichung (47) ist offenbar die Verallgemeinerung des Falles d ungerade aus Abschnit 2.
Der Fall d gerade läßt sich hingegen nicht so glatt auf die ganz allgemeine Situation übertragen. Es gib folgendes Beispiel : Seien p=2 und die folgende Zerlegung des R^4 gegeben

$$E_0 = R[(1,-1,1,-1),(1,-1,-1,1)] \ , \ E_1 = R(1,1,1,1) \ , \ E_2 = R(1,1,-1,-1)$$

dann teilt 2 alle $det(\Delta_i)$ für $i = 0,1,2$; die Codes C_i und C_{ij} sind

$$C_1 = C_2 = \{0000, 1111\}$$

$$C_{01} = C_{02} = LinSpan_{F_2}[1100, 1010, 1001]$$

und infolgedessen sind die beiden folgenden Durchschnitte leer :

$$(C_{01} - C_1) \cap C_2 = \emptyset \quad C_1 \cap (C_{02} - C_2) = \emptyset$$

Sogar die Folgerung mit Gleichung (13) in dem speziellen Fall $E_0 = R(1,1,...,1)$ kann man nicht auf ungerade Primzahlen p übertragen. Es gilt zwar :
Folgerung: Für eine Primzahl p mit p teilt d ist höchstens einer der beiden folgenden Durchschnitte nichtleer :

$$(C_{01} - C_1) \cap C_2 \quad \text{oder} \quad C_1 \cap (C_{02} - C_2) \tag{48}$$

Dazu lassen wir zunächst $R^p = F_0 \perp F_1$ mit $F_0 = R(1,1,...,1)$ und $F_1 = LinSpan_R[e_i - e_j \mid 1 \leq i < j \leq n]$. Wie in Abschnitt 2 setzen wir dann

$$R^{pn} = R^p \otimes R^n = T_{00} \perp (T_{01} \perp T_{12}) \perp (T_{02} \perp T_{11}) \perp T_{10}$$

mit $T_{ij} = F_i \otimes E_j$ und $T_1 = T_{01} \perp T_{12}$ sowie $T_2 = T_{02} \perp T_{11}$. Falls nun etwa

$$(C_{01} - C_1) \cap C_2 \neq \emptyset$$

ist, so gibt es Vektoren $v \in \Delta_{01}$ und $w \in \Delta_2$ mit $\bar{v} = \bar{w}$ und mit $< v, u >= \phi(E_1)$. Dann ist der Vektor

$$x = \frac{1}{p}(u \otimes v \ + \ (p \cdot e_1 - u) \otimes w) \quad \in \quad T_0 \perp T_1$$

ganzzahlig und zeigt $\phi(T_1)$ teilt $\phi(E_1)$ und somit folgt

$$\phi(T_1) = \phi(E_1) \ \text{ und } \ \phi(T_2) = 2 \cdot \phi(E_2)$$

Genauso für den zweiten Durchschnitt . Aus der Produktformel für die Totientenzahlen erhält man deshalb die Folgerung. □

Es kann aber sein, daß auch im Falle p teilt d beide Durchschnitte in (48) leer sind, wie das folgende Beispiel zeigt:
Sei $p = 3$ und $d = 9$ und setze

$$E_0 = R(1,1,1,1,1,1,1,1,1)$$

$$E_1 = R[(2,2,2,-1,-1,-1,-1,-1,-1),(1,0,0,-1,0,0,0,0,0)]$$

$$E_2 = \text{ orthogonales Komplement von } E_0 \perp E_1 \text{ in } R^9$$

Dann ist $C_{02} \cap C_1 = C_0 \subset C_2$ und somit $C_1 \cap (C_{02} - C_2) = \emptyset$ sowie auch $(C_{01} - C_1) \cap C_2 = \emptyset$, wie man mit Hilfe der „ parity-check "-Gleichungen

$$x_1 - x_4 = 0\ ,\ x_1 + x_2 + x_3 = 0\ ,\ x_4 + x_5 + x_6 + x_7 + x_8 + x_9 = 0$$

für C_2 leicht erkennen kann .

5 Switching-äquivalente Graphen und Graphen mit denselben Parametern

In diesem Abschnitt wollen wir eine Reihe von Bemerkungen über verschiedene stark reguläre Graphen mit denselben Parametern wie $V^{\pm}(2h)$ machen, welche die Berechnung der Totientenzahlen aus dem vorliegenden Satz verdeutlichen und relativieren.
Bemerkung 1 : Es gibt stark reguläre Graphen mit denselben Parametern wie $V^{+}(2h)$ und den Totientenzahlen

$$\phi(E_1) = \phi(E_2) = 2^h$$

Für $h > 3$ kann man solche Graphen finden, die nicht switching-äquivalent mit $V^{+}(2h)$ sind. Eine analoge Bemerkung gilt auch für $V^{-}(2h)$.
Bemerkung 2 : Es gibt stark reguläre Graphen mit denselben Parametern wie $V^{+}(2h)$ und sogar switching-äquivalent zu $V^{+}(2h)$ mit den Totientenzahlen

$$\phi(E_1) = 2 \quad \textit{und} \quad \phi(E_2) = 2^{2h-1}$$

mit der entsprechenden Numerierung der Eigenräume wie bei $V^{+}(2h)$.

In der Arbeit [Y] wurde ein Resultat besprochen, das in einem gewissen Zusammenhang mit den vorliegenden Betrachtungen steht. Weil nun die Methoden in der zitierten Arbeit wesentlich zu umständlich sind, wollen wir die Gelegenheit ergreifen, die Grundzüge einer Vereinfachung für die Beweise von [Y] anzugeben. Gleichzeitig wird sich dabei eine Verallgemeinerung ergeben, die dortselbst nicht beachtet worden ist, die aber im Zusammenhang mit der Arbeit [Sh] doch von einer gewissen Wichtigkeit ist.

Wir betrachten dazu also auf dem F_2-Vektorraum $V = F_2^{2h}$ eine nichtausgeartete Bilinearform $B : V \times V \rightarrow F_2$ und wir versehen $V_0 = V - \{0\}$ mit der Struktur eines stark regulären Graphen, indem wir $\{x, y\}$ mit $B(x, y) = 0$ als Kanten betrachten. Dann gilt :

Bemerkung 3: Die maximale Zahl von unabhängigen Punkten in V_0 ist $2h+1$. Dies ist vollständig elementar und wurde auch in [Y] bemerkt, aber ganz am Ende (Abschnitt 8) als ein gewisser Zusatz. Für den an Einfachheit und Klarheit Interesierten ist dies jedoch der Ausgangspunkt.

Sei nun irgendein Graph G aus der Switchingklasse von $V^{\pm}(2h)$ gegeben, und sei $K_{a,b}$ irgendein induzierter vollständig-bipartiter Untergraph von G . Durch Seidel-Switching kann man dann das Isolieren irgendeines Punktes aus $K_{a,b}$ erreichen. Der geswitchte Gesamtgraph G_s wird dann aus einem isolierten Punkt p zusammen mit einer Kopie des Graphen V_0 bestehen. $K_{a,b} - \{p\}$ ist eine Menge von unabhängigen Punkten in V_0 und als solche ist ihre Kardinalität durch $2h + 1$ beschränkt. Es gilt also

$$a + b \leq 2h + 2$$

für jeden vollständig-bipartiten Untergraphen $K_{a,b}$ von G. Insbesondere trifft dies auf die Graphen $V^{\pm}(2h)$ zu. Durch eine entsprechende Verfeinerung dieses Argumentes, die wir hier nicht ausführen wollen, kann man alle maximalen $K_{a,b}$ in $V^{\pm}(2h)$ und in deren Unterkomponenten $Alt^{\pm}(2h)$ und $Sym_0^{\pm}(2h)$ bestimmen, ohne die Resultate von [Sh] oder gar den Nichtexistenzsatz von linear unabhängigen Vektorfeldern auf Sphären verwenden zu müssen, wie dies ja leider in [Y] geschehen ist.

Ein gewisser Zusammenhang mit den Totientenzahlen besteht nun darin, daß für $V^{\pm}(2h)$ die Menge der unabhängigen Punkte, deren maximale Zahl c ist, im Falle $c = 2^h$ eine reguläre Menge [B2] bildet, was wiederum $\phi(E_1) = 2^h$ zur Folge hat.

[B1] T. Bier A Product Formula for Euler's Totient , Bull LMS 17(1985)527-530

[B2] T. Bier , P.K. Chua Numerical Invariants of Strongly Regular Graphs JCT(A) 49(1988)145-171

[B3] T. Bier Totient Numbers of an Arithmetic Progression in a Hypercube : The Case of Step Length 2 EJC 12(1991)91-94

[B4] T. Bier Clifford-Gitter ,186 Seiten,Manuskript Göttingen 1984 , als Habilitationsschrift abgelehnt vom Mathematischen Institut der Georg-August-Universität Göttingen 1987

[B5] T. Bier A Remark on the Construction of Normed and Nonsingular bilinear maps , Proceedings of the Japan Academy 56(1983)328-330

[B6] T. Bier Totient Numbers of an Arithmetic Progression in a Hypercube: The Coprime Case EJC 11(1990)319-321

[D] P. Delsarte Pairs of Vectors in the Space of an Association Scheme Philips Research Reports
[Q] D. Quillen The Cohomology Rings of Extraspecial Twogroups and the Spinor groups Math. Ann. 194(1971) 197-212
[S1] J.J. Seidel Strongly Regular Graphs , Proc. 7th British Comb. Conf. LMS Lect. Note Ser.38 (1979)157-180
[S2] J.J. Seidel , A Survey on Twographs , Academia Naz. Lincei , Rom 1973 Proc. Int. Coll. Teorie Combinatorie I (1976) 481-511
[Sh] D.B. Shapiro Spaces of Similarities I , the Hurwitz Problem, Journal of Algebra 46 (1977) 148-170
[Y] P.Y.H. Yiu , Strongly Regular Graphs and Hurwitz-Radon Numbers , Graphs and Combinatorics 6(1990)61-69

Dr Thomas Bier
z. Z. Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D 5300 Bonn
Deutschland

Am Badepark 16
D 2903 Bad Zwischenahn
Deutschland