12.2 Kombinatorische Designs

Designs sind kombinatorische Strukturen, die aus der statistischen Versuchsplanung (design of experiments) und aus der Geometrie stammen, auch Systemtips im Lotto gehören dazu. Sie werden mit Hilfe von Parameterquadrupeln $t, v, k, \lambda \in \mathbb{N}^*$ beschrieben, so daß sich u.a. auch die Frage stellt, zu welchen Parameterquadrupeln Designs existieren.

Bei entsprechenden Untersuchungen spielten in jüngster Zeit Verbandsoperationen eine zentrale Rolle, diese werden jetzt bechrieben. Dabei gelang u.a. die weltweit erste Konstruktion eines 7-Designs ($t = 7$) mit kleinen Parametern durch die Verwendung einer Matrix $A^\wedge$, im Zusammenspiel mit einer modernen Implementierung des LLL-Algorithmus zur Lösung diophantischer Gleichungen.

12.2.1 Definition ($t-(v,k,\lambda)$-Design) Ein $t-(v,k,\lambda)$-*Design* ist eine Teilmenge

$$\mathcal{B} \subseteq \binom{v}{k}$$

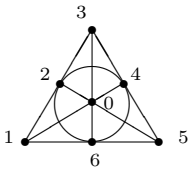
der Menge der k-Teilmengen einer Menge v von *Punkten*. Die Elemente $B \in \mathcal{B}$ heißen *Blöcke*, und die *Parameter* t, v, k und λ müssen den folgenden Bedingungen genügen:

$$\forall\, T \in \binom{v}{t} \colon \; \big|\, \{B \in \mathcal{B} \mid T \subseteq B\} \,\big| = \lambda,$$

d.h. jede t-Teilmenge der Punktemenge liegt in genau λ Blöcken. •

12.2.2 Beispiele aus der Geometrie sind die projektiven Ebenen.

i) Hier zunächst ein gut bekannter Spezialfall, die *Fanoebene,*



Hierbei ist

$$\mathcal{B} = \{\{1,2,3\},\{3,4,5\},\{5,6,1\},\{0,1,4\},\{0,2,5\},\{0,3,6\},\{2,4,6\}\},$$

$v = 7$, $k = 3$. Die Fanoebene ist ein 1-Design mit $\lambda = 3$, und sie ist auch ein 2-Design mit $\lambda = 1$.

ii) Wie die Fanoebene sind sämtliche *projektiven Ebenen* 2-Designs mit $\lambda = 1$ (und der Zusatzbedingung, daß je zwei Blöcke genau einen Punkt gemeinsam haben). Genauer: Die klassischen projektiven Ebenen sind, für Primzahlpotenzen q, $2-(q^2+q+1, q+1, 1)$–Designs. ◇

Die Designs auf der Punktemenge v kann man mit Hilfe der *Inzidenzmatrix* $M^v_{t,k}$ beschreiben, deren Zeilen zu den $T \in \binom{v}{t}$ gehören, die Spalten zu den $K \in \binom{v}{k}$. Die Einträge m^v_{TK} von $M^v_{t,k}$ sind wie folgt definiert:

$$m^v_{TK} := \begin{cases} 1, & \text{falls } T \subseteq K, \\ 0, & \text{sonst.} \end{cases}$$

Ein $t-(v,k,\lambda)$-Design $\mathcal{B}$ ist dann eine Auswahl geeigneter Spalten dieser Matrix:

12.2.3 Folgerung *Die Menge aller $t-(v,k,\lambda)$-Designs auf v ist die Menge der Blöckemengen $\mathcal{B}$, die man aus den 0-1-Lösungen x des linearen Gleichungssystems*

$$M^v_{t,k} \cdot x = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}$$

wie folgt bekommt:

$$\mathcal{B} := \Big\{ B \in \binom{v}{k} \;\Big|\; x_B = 1 \Big\}.$$

□

$M^v_{t,k}$ ist eine $\binom{v}{t} \times \binom{v}{k}$-Matrix, und die Ermittlung von 0-1-Lösungen ist ein schwieriges Problem. Nach der Konstruktion der ersten 6-Designs versuchte man lange vergeblich, 7-Designs mit moderaten Parametern zu finden (solche mit "astronomischen" Parametern waren aus einem Existenzsatz von Teirlinck seit 1987 bekannt). Es bestand bald die Vermutung, daß es womöglich 7-Designs mit $v = 33$ und $k = 8$ geben könne. In diesem Fall hat die Inzidenzmatrix etwa $6 \cdot 10^{13}$ Einträge, λ war unbekannt, es war (und ist) aber zur Zeit unmöglich, 0-1-Lösungen für derart große Systeme zu finden.

Der "Trick" war (und ist) es, zur Reduktion des Problems weitere Bedingungen an die Designs zu stellen, die wir konstruieren wollen. Als sehr wirksam hat sich die Methode erwiesen, *eine Untergruppe $G \leq S_v$ vorzugeben, die in der Automorphismengruppe enthalten sein soll.* Das ist natürlich riskant, denn oft wird es keine Designs mit dieser Eigenschaft geben. Andererseits reduziert man den Suchraum und die Datenmenge ganz gewaltig. Hinzukommt, daß diese Methode auch bei anderen Strukturen verwendbar ist, z.B. bei der Suche nach linearen Codes mit vorgegebener Minimaldistanz (M. Braun und A.Kohnert haben auf diese Weise mehrere Hundert Codes gefunden mit besseren Parametern als bisher bekannt).

Im Fall der 7-Designs hatte man tatsächlich eine Gruppe "in Verdacht", konnte aber das entsprechende Gleichungssystem nicht lösen, was dann hier in Bayreuth 1995 gelungen ist. Seitdem konnte mit dieser Methode die Existenz von $t-(v,k,\lambda)$-Designs für Tausende neuer Parameterquadrupel (t,v,k,λ) nachgewiesen werden (R. Laue).

Ein Element $\pi \in S_v$ heißt *Automorphismus* des Designs $\mathcal{B}$, wenn gilt

$$\pi\mathcal{B} := \big\{ \pi B := \{\pi b \mid b \in B\} \;\big|\; B \in \mathcal{B} \big\} = \mathcal{B}.$$

Jede Untergruppe $G \leq S_v$, die aus solchen Automorphismen besteht, heißt *eine* Gruppe von Automorphismen des Designs, und die Gruppe aller dieser Automorphismen heißt *die* oder die *volle* Automorphismengruppe:

$$Aut(\mathcal{B}) := \{\pi \in S_v \mid \pi\mathcal{B} = \mathcal{B}\}.$$

Die Aufgabe ist also die Berechnung von mindestens einem $t-(v,k,\lambda)$-Design, das G in seiner vollen Automorphismengruppe enthält und, wenn möglich, alle solchen $t-(v,k,\lambda)$-Designs zu ermitteln und zu klassifizieren. Natürlich hätte man auch gerne all diejenigen Designs bestimmt, die G als *volle* Automorphismengruppe haben.
Um diese Probleme in die Reichweite heutiger PCs zu bringen, betrachten wir, anstelle von $M^v_{t,k}$, eine weit kleinere Matrix, die mit Hilfe von G gewonnen wird. *Diese Matrix ist eine Teilmatrix der Matrix $A^\wedge$ zur Verbandsoperation ${}_G(2^v, \cap, \cup)$, die oben schon erwähnt wurde*:

$$M^G_{t,k} := (m^G_{T,K}), \text{ mit } m^G_{T,K} := |\{K' \in G(K) \mid T \subseteq K'\}|,$$

T durchläuft dabei eine Transversale von $G \setminus\!\setminus \binom{v}{t}$, K eine Transversale von $G \setminus\!\setminus \binom{v}{k}$.

Es sei jetzt daran erinnert, daß die Berechnung solcher Transveralen via Doppelnebenklassentransveralen erfolgen kann: S_v operiert transitiv auf $\binom{v}{k}$ und auf $\binom{v}{t}$, wir erhalten also — über das Fundamentallemma — Bijektionen

$$G \setminus\!\setminus \binom{v}{k} \to G\backslash S_v / S_k \oplus S_{v\backslash k}\,,\; G(\gamma K) \mapsto G\gamma(S_k \oplus S_{v\backslash k}),$$

wobei $K := \{0, 1, \ldots, k-1\} \in \binom{v}{k}$, $S_k \oplus S_{v\backslash k}$ der Stabilisator von K, $\gamma \in S_v$.
Ganz entsprechend haben wir auch

$$G \setminus\!\setminus \binom{v}{t} \to G\backslash S_v / S_t \oplus S_{v\backslash t}\,,\; G(\gamma T) \mapsto G\gamma(S_t \oplus S_{v\backslash t}).$$

Man kann also aus Transversalen dieser Mengen von Doppelnebenklassen Transversalen der Bahnen von G auf den k– und auf den t–Teilmengen gewinnen, also die Spaltenindizes K und die Zeilenindizes T der gesuchten Matrix $M^G_{t,k} := (m^G_{T,K})$, samt den entsprechenden Einträgen.

Spielentscheidend sind dabei Methoden, Transversalen von solchen Doppelnebenklassenmengen

$$G\backslash S_v / S_t \oplus S_{v-t}$$

sukzessive nach ansteigendem t zu berechnen (das *Leiterspiel*).

Weil G in der Automorphismengruppe liegen soll, besteht jedes Design $\mathcal{B}$ aus vollen Bahnen von G auf $\binom{v}{k}$, und weil G die Inklusion von t– in k–Teilmengen erhält, gilt

12.2.4 Der Satz von Kramer und Mesner *Die Menge aller $t-(v,k,\lambda)$-Designs mit $G \leq S_v$ als Gruppe von Automorphismen ergibt sich aus der Menge der 0-1-Lösungen x von*

$$M_{t,k}^{G} \cdot x = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}.$$

□

12.2.5 Beispiel Betrachten wir zunächst ein Beispiel mit den sehr kleinen Parametern $t := \lambda := 1$, $v := 4$ und $k := 2$. Wegen

$$\binom{4}{2} = \big\{\{0,1\},\{0,2\},\{0,3\},\{1,2\},\{1,3\},\{2,3\}\big\}$$

und

$$\binom{4}{1} = \big\{\{0\},\{1\},\{2\},\{3\}\big\}$$

ergibt sich als Inzidenzmatrix

$$M_{t,k}^{v} = M_{1,2}^{4} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Schreibt man jetzt als Zusatzbedingung die folgende Gruppe von Automorphismen vor:

$$G := \langle (0123) \rangle,$$

eine Untergruppe der Ordnung 4 in S_4, dann ergeben sich die Bahnenmengen

$$G \setminus\!\setminus \binom{4}{2} = \Big\{\big\{\{0,1\},\{0,3\},\{1,2\},\{2,3\}\big\},\big\{\{0,2\},\{1,3\}\big\}\Big\},$$

und

$$G \setminus\!\setminus \binom{4}{1} = \big\{\{0\},\{1\},\{2\},\{3\}\big\}.$$

Diese Bahnenmengen entsprechen den Spalten bzw. den Zeilen der Kramer–Mesner–Matrix

$$M_{t,k}^{G} = M_{1,2}^{G} = \begin{pmatrix} 2 & 1 \end{pmatrix}.$$

Aus der Inzidenzmatrix mit 12 Elementen ist also eine Kramer–Mesner–Matrix mit nur noch 2 Einträgen geworden, und man sieht sofort, daß das lineare Gleichungssystem

$$M_{1,2}^{G} \cdot x = \begin{pmatrix} 2 & 1 \end{pmatrix} \cdot x = (\lambda)$$

für $\lambda = 1$ genau eine Lösung hat,

$$x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Das entsprechende Design ist

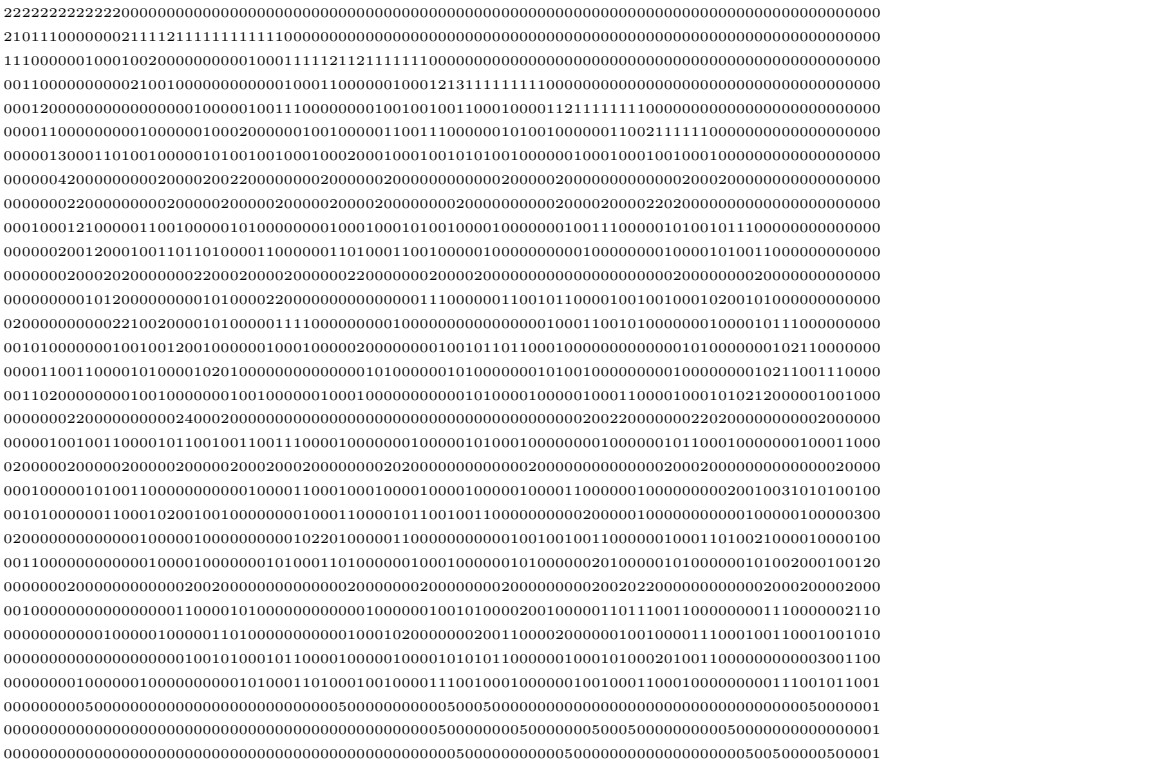
$$\mathcal{B} = \{\{0,2\},\{1,3\}\}.$$

Demnach existiert genau ein $1-(4,2,1)$-Design mit G als einer Gruppe von Automorphismen. (Weil G, als Gruppe der Ordnung 8, maximal in S_4 ist und S_4 offenbar *nicht* in der Automorphismengruppe liegt, ist G sogar die *volle* Automorphismengruppe dieses Designs.) ◇

Das historisch erste 7-Design mit moderaten Parametern, das gefunden wurde, war ein $7-(33,8,10)$-Design mit $G = \mathrm{P\Gamma\,L}_2(32)$, einer Untergruppe von S_{33} mit den Erzeugenden

$$\begin{aligned}\alpha &= (0)(1\,2\,4\,8\,16)(3\,6\,12\,24\,17)(5\,10\,20\,9\,18)(7\,14\,28\,25\,19)\\ &\quad (11\,22\,13\,26\,21)(15\,30\,29\,27\,23)(31)(32)\\ \beta &= (1\,18\,30)(2\,21\,12)(3\,10\,28)(4\,31\,32)(5\,24\,14)(6\,7\,17)(8\,25\,27)\\ &\quad (9\,19\,20)(11\,15\,13)(16\,23\,29)(22\,0\,26).\end{aligned}$$

Die Kramer–Mesner–Matrix, die bereits Magliveras und Leavitt bekannt war, und die von A. Betten erneut und mit Hilfe von Doppelnebenklassen berechnet wurde, ist



Sie hat um den *Faktor* 10^{10} weniger Einträge als die Inzidenzmatrix, so daß mit der verbesserten Implementierung des LLL-Algorithmus durch A. Wassermann die folgenden beiden Lösungen des Gleichungssystems mit $\lambda = 10$ und $\lambda = 16$ gefunden werden konnten:

00111000101001001100011010000100100000001011011000101111000000010010010100001101110110010101110001100011101011011001110010111011011111110100100111010000111111101101101011110010001001101010001111

Es zeigte sich später, daß es insgesamt 4 996 426 0-1-Vektoren x gibt, die das System für $\lambda = 10$ lösen. In der Zwischenzeit sind auch 8-Designs, 9-Designs ... gefunden worden.