2.7 Golay-Codes

Ein t-(v,k,λ)-*Design* ist ein Paar $(P,\mathfrak{B})$ bestehend aus einer Menge von *Punkten* P und einer Menge $\mathfrak{B}$ von *Blöcken* $B \subseteq P$ mit folgenden Eigenschaften:

(i) $|P| = v$,

(ii) $|B| = k$ für jedes $B \in \mathfrak{B}$, und:

(iii) Zu jedem $X \subseteq P$ mit $|X| = t$ gibt es genau λ Blöcke $B \in \mathfrak{B}$ mit $X \subseteq B$.

Designs sind wichtige Objekte der diskreten Mathematik, spielen für uns jedoch nur eine kleine Nebenrolle zur Beschreibung des sogenannten *binären Golay-Codes*.

Man betrachte den Körper $\mathbb{Z}_{11}$. Die Menge $D := \{0,2,6,7,8,10\}$ bildet eine sogenannte $(11,6,3)$-*Differenzenmenge*, das heißt jedes $x \in \mathbb{Z}_{11} \setminus \{0\}$ läßt sich auf genau 3 Weisen als Differenz zweier Elemente aus D darstellen. Das prüft man anhand der 6×6-Differenzentabelle von Hand nach (eingetragen ist die Differenz von Zeilen- und Spaltenindex):

	0	2	6	7	8	10
0	0	9	5	4	3	1
2	2	0	7	6	5	3
6	6	4	0	10	9	7
7	7	5	1	0	10	8
8	8	6	2	1	0	9
10	10	8	4	3	2	0

Die elf durch zyklisches Verschieben von D entstehenden Mengen

$$D + j := \{d + j : d \in D\},\ j \in \mathbb{Z}_{11},$$

bilden die Menge $\mathfrak{B}$ der Blöcke eines $2-(11,6,3)$-Designs auf der Punktmenge $P = \mathbb{Z}_{11}$, das heißt: Jeder Block enthält 6 Punkte und je zwei Punkte $x \neq y$ aus P sind gemeinsam in genau drei Blöcken aus $\mathfrak{B}$ enthalten: Ist nämlich $x \neq y$ aus P fest und $x, y \in D + i$, so folgt $x = d + i$ und $y = d' + i$ für geeignete $d, d' \in D$, also $d - d' = (x - i) - (y - i) = x - y$, was genau drei Lösungen (d, d') in $D \times D$ hat; die ersten Komponenten dieser drei Lösungen müssen paarweise verschieden sein, so daß sich daraus genau drei Lösungen für $i = x - d$ ergeben. — Umgekehrt ist jeder Punkt $x \in P$ in genau 6 Blöcken enthalten, nämlich in den Blöcken $D + (x - d)$ für $d \in D$, und je zwei Blöcke haben genau drei Punkte gemeinsam: Sind nämlich $i \neq j$ fest und $x \in (D + i) \cap (D + j)$, so gilt $x = d + i$ und $x = d' + j$ für gewisse $d, d' \in D$, also $d - d' = (x - i) - (x - j) = j - i$, was genau drei Lösungen (d, d') in $D \times D$ besitzt, woraus sich wiederum genau drei Lösungen für $x = d + i$ ergeben.

Betrachte man nun die durch

$$N(i,x) := \begin{cases} 1 & \text{falls } x \in D + i \\ 0 & \text{sonst} \end{cases}$$

gegebene 11×11-Block-Punkt-Inzidenzmatrix über $\mathbb{Z}_2$. Konkret ist das:

$$N = \begin{pmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1
\end{pmatrix}$$

Zeilen und Spalten denkt man sich mit $\mathbb{Z}_{11}$ indiziert, so daß in der in der 0-ten Zeile in Spalte s genau dann eine 1 steht, wenn $s \in D$ ist. Die Konstruktion bringt es mit sich, daß die folgenden Zeilen sich durch zyklische Rotation nach rechts ergeben. Infolge der oben abgeleiteten Eigenschaften des korrespondierenden Designs findet man in jeder Zeile und jeder Spalte genau 6 Einträge 1, und je zwei Zeilen — wie auch je zwei Spalten — haben an genau drei gemeinsamen Stellen den Eintrag 1. (Tatsächlich kann man sich — von Hand — überlegen, daß es bis auf den Tausch von Zeilen oder Spalten nur eine solche Matrix gibt.) Man überzeugt sich leicht davon, daß die Summe zweier Zeilen genau 6 Einsen enthält.

Nun betrachte man die 12×12-Matrix $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & N \end{smallmatrix}\right)$, das heißt die erste Zeile wie auch Spalte besteht aus einer 0 gefolgt von 11 Einträgen 1, und sodann die 12×24-Matrix $G := (E_{12}\, P)$ über $\mathbb{Z}_2$:

$$G = \left(\begin{array}{cccccccccccc|cccccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1
\end{array}\right)$$

(Die Trennlinie grenzt E_{12} von P ab.) Je zwei Zeilen von G haben an 6 oder an 4 Stellen gemeinsame Einsen, das heißt ihr inneres Produkt ist gleich 0. Hieraus folgt, daß die Summe beliebig vieler Zeilen eine durch 4 teilbare Anzahl Einträge 1 hat: Ist dies nämlich für die Summe $g = g_1 + \cdots + g_n$ bewiesen und g_{n+1} eine weitere Zeile, und bezeichnen A, B, C die Mengen der Stellen, an denen g

bzw. g_{n+1} bzw. $g + g_{n+1}$ den Eintrag 1 haben, so ist

$$gg_{n+1}^\top = (g_1 + \cdots + g_n)g_{n+1}^\top = \sum_{i=1}^{n} g_i g_n^\top = 0,$$

also haben g und g_{n+1} an einer geraden Anzahl von Stellen gemeinsame Einsen; man liest $|B| \equiv 0$ modulo 4 an der Matrix G ab und erhält $|C| = |A \setminus B| + |B \setminus A| = |A| + |B| - 2|A \cap B| \equiv 0 + 0 - 2|A \cap B| \equiv 0$ modulo 4.

Tatsächlich kann die Summe $g = g_1 + \cdots + g_n$ irgendwelcher Zeilen von G nicht genau vier Einträge 1 haben (im Fall $n > 4$ werden bereits an den 12 führenden Stellen mehr als 4 Einsen in der Summe beigetragen, im Fall $n \in \{1, 2\}$ erhält man wenigstens 6 Einsen an den letzten 11 Stellen, im Fall $n = 0$ gar keine Einsen, und die Fälle $n \in \{3, 4\}$ erledigt man durch Fallunterscheidung mit der Beobachtung, daß die Summe dreier oder vierer Zeilen von N (!) nicht 0 ist). Folglich hat der von G erzeugte $[24, 12]$-Code C, ein sogenannter *erweiterter binärer Golay-Code*, den Minimalabstand $d(C) = 8$. Streicht man in der Generatormatrix G (zum Beispiel) die letzte Spalte, so erzeugt die neue Matrix einen $[23, 12]$-Code mit Minimalabstand 7, einen sogenannten *binären Golay-Code*. Er ist 3-fehlerkorrigierend, die Hamming-Schranke ist $2^{23}/(\binom{23}{0}+\binom{23}{1}+\binom{23}{3}+\binom{23}{3}) = 2^{23}/2048 = 2^{12}$ also *gleich* $|C|$. Daher ist C perfekt 3-fehlerkorrigierend.

Dieser Code ist ein absoluter Ausnahmecode unter den binären Codes, wie der folgende Satz zeigt.

Satz 12 *Genau dann gibt es einen perfekt 3-fehlerkorrigierenden n-Code über $\mathbb{Z}_2$, wenn $n = 7$ oder $n = 23$ ist.*

Beweis. Der 7-Wiederholungscode C über $\mathbb{Z}_2$ ist ein perfekt 3-fehlerkorrigierender 7-Code, denn $|B_3(0)| = \binom{7}{0} + \binom{7}{1} + \binom{7}{2} + \binom{7}{3} = 1 + 7 + 21 + 35 = 64$ und $|C| = 2 = 2^7/64$. Der binäre Golay-Code ist ein perfekt 3-fehlerkorrigierender 23-Code.

Sei nun umgekehrt C ein binärer perfekt 3-fehlerkorrigierender n-Code. Dann gilt

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} = 2^\ell$$

für eine Zahl $\ell \geq 0$, da sonst die Hamming-Schranke nicht erreicht werden kann. Schreibt man die Binomialkoeffizienten als Brüche $\frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{k(k-1)\cdot\cdots\cdot3\cdot2\cdot1}$ und bringt sie auf den Hauptnenner 6, so erhält man durch Faktorisierung der Zählersumme und Multiplikation mit 6 die Gleichung

$$(n+1)(n^2 - n + 6) = (n+1)((n+1)^2 - 3(n+1) + 8) = 3 \cdot 2^{\ell+1}.$$

Ist $n + 1$ durch 16 teilbar, so ist $a := (n+1)^2 - 3(n+1) + 8$ nicht durch 16, aber durch 8 teilbar und folglich gleich 8 oder 24 (die Primfaktorzerlegung von a ist ja $2^\alpha 3^\beta$ mit $\alpha = 3$ und $\beta \leq 1$); $n^2 - n + 6 = 8$ liefert $n(n-1) = 2$, also $n = 2$,

$n^2 - n + 6 = 24$ dagegen $n(n-1) = 18$, in beiden Fällen den Widerspruch zu $n \geq 16$. Folglich ist $n+1$ nicht durch 16 teilbar, die Primfaktorzerlegung von $n+1$ also $2^\alpha 3^\beta$ mit $\alpha \leq 3$ und $\beta \leq 1$ und somit $n+1$ ein Teiler von 24. Der Minimalabstand erzwingt $n \geq 7$, also $n+1 \geq 8$ und somit $n+1 \in \{8, 12, 24\}$, also $n \in \{7, 11, 23\}$. Für $n = 11$ erhält man $n^2 - n + 6 = 116$, also $29 | 3 \cdot 2^{\ell+1}$, Widerspruch. □

Sei C die wie in Satz 5 für $q = 5$ definierte symmetrische 6×6-Konferenzmatrix über $\{0, +1, -1\}$ und $G = (E_6\, Q)$, also:

$$\left(\begin{array}{cccccc|cccccc} + & 0 & 0 & 0 & 0 & 0 & 0 & + & + & + & + & + \\ 0 & + & 0 & 0 & 0 & 0 & + & 0 & + & - & - & + \\ 0 & 0 & + & 0 & 0 & 0 & + & + & 0 & + & - & - \\ 0 & 0 & 0 & + & 0 & 0 & + & - & + & 0 & + & - \\ 0 & 0 & 0 & 0 & + & 0 & + & - & - & + & 0 & + \\ 0 & 0 & 0 & 0 & 0 & + & + & + & - & - & + & 0 \end{array}\right)$$

Dabei stehen $+$ und $-$ für $+1$ bzw. -1. Aus der definierenden Eigenschaft für Konferenzmatrizen erhalten wir die Gleichung $GG^\top = E_6 + 5E_6 = 6E_6$. Wir fassen G als Matrix über $\mathbb{Z}_3$ und dort gilt $GG^\top = 6E_6 = 0$. Wir bezeichnen die (offensichtlich linear unabhängigen) Zeilen von G mit $g_1, \ldots, g_6$. Ist nun

$$x = \sum_{i=1}^{6} \lambda_i g_i$$

ein Wort aus dem von diesen erzeugten Code C, so gilt wegen $g_i g_j^\top = 0$ für alle i, j aus $\{1, \ldots, 6\}$ auch

$$xx^\top = \sum_{i=1}^{6} \sum_{j=1}^{6} \lambda_i \lambda_j g_i g_j^\top = 0.$$

Folglich ist $d(x, 0)$ durch 3 teilbar. Ist $x = \lambda_i g_i + \lambda_j g_j$ für $\lambda_i, \lambda_j \neq 0$, so ist $d(x, 0) \geq 2 + 2$ und $d(x, 0) \leq 8$, also $d(x, 0) = 6$ und daher $x_\ell = 0$ für genau zwei Stellen ℓ aus $\{7, \ldots, 12\}$. Daher ist auch im Fall $x = \lambda_i g_i + \lambda_j g_j + \lambda_k g_k$ für $\lambda_i, \lambda_j, \lambda_k \neq 0$ $d(x, 0) \geq 2 + 2$ und somit $d(x, 0) \geq 4$ für *alle* $x \in C$, also $d(x, 0) \geq 6$ für alle $x \in C$. Streicht man eine beliebige Spalte (meist wird die 7te gewählt), so erhält man einen $[11, 6]$-Code über $\mathbb{Z}_3$ mit Minimalabstand 5. Es ist $|B_2(0)| = \binom{11}{0}2^0 + \binom{11}{1}2^1 + \binom{11}{2}2^2 = 1 + 22 + 55 \cdot 4 = 243 = 3^5$, die Hamming-Schranke also gleich $3^{11}/3^5 = 3^6 = |C|$, folglich ist C perfekt 2-fehlerkorrigierend. Man nennt C einen *ternären Golay-Code*.

Ohne Beweis: Nennt man die binären $(2r+1)$-Wiederholungscodes die *trivialen* perfekt r-fehlerkorrigierenden Codes, so ist der binäre Golay-Code der einzige nichttriviale binäre perfekt r-fehlerkorrigierenden Code für $r > 1$ und der einzige nichttriviale perfekt r-fehlerkorrigierende Code für $r > 2$ überhaupt. Ist q eine Primzahlpotenz, so ist der ternäre Golay-Code der einzige nichttriviale q-adische perfekt 2-fehlerkorrigierende Code. Es ist offen, für welche q es weitere nichttriviale q-adische perfekt 2-fehlerkorrigierende Codes gibt.