RWTH AACHEN UNIVERSITY

Extremale Codes und Blockdesigns

Seminarausarbeitung

Sebastian Piper

Dozent: Prof. Dr. Gabriele Nebe
Aachen, den 15.08.2011

Inhaltsverzeichnis

1 Codes und Gewichtszähler 2

2 Extremale Codes und Blockdesigns 7

3 Der erweiterte binäre Golay-Code 17

Literatur 22

1 Codes und Gewichtszähler

Definition 1. Sei p eine Primzahl, $q = p^k$ für $k \in \mathbb{N}$ und $N \in \mathbb{N}$. Ein linearer Code $\mathcal{C}$ über $\mathbb{F}_q$ der Länge N ist ein linearer Teilraum $\mathcal{C} \leq \mathbb{F}_q^N$.

Definition 2. Sei $\mathcal{C} \leq \mathbb{F}_q^N$ ein linearer Code der Länge N.

i) Der duale Code von $\mathcal{C}$ ist definiert als der Orthogonalraum

$$\mathcal{C}^\perp = \left\{x \in \mathbb{F}_q^N | x \cdot c = 0 \; \forall c \in \mathcal{C}\right\}$$

von $\mathcal{C}$ bzgl. der nicht ausgearteten symmetrischen Bilinearform

$$x \cdot c := \sum_{i=1}^{N} x_i y_i.$$

ii) Das Gewicht eines Codewortes $c \in \mathcal{C}$ ist

$$wt(c) := \left|\{i \in \{1, \ldots, N\} | c_i \neq 0\}\right|.$$

iii) Das Minimalgewicht von $\mathcal{C}$ ist

$$d(\mathcal{C}) := \min\{wt(c) | 0 \neq c \in \mathcal{C}\}.$$

iv) Der vollständige Gewichtszähler $p_\mathcal{C} \in \mathbb{C}[x_0, \ldots, x_{q-1}]$ von $\mathcal{C}$ ist definiert als

$$p_\mathcal{C}(x) := \sum_{c \in \mathcal{C}} \prod_{i=1}^{N} x_{c_i}.$$

v) Der Hamming Gewichtszähler $h_\mathcal{C} \in \mathbb{C}[x, y]$ von $\mathcal{C}$ ist definiert als

$$h_\mathcal{C}(x, y) := \sum_{c \in \mathcal{C}} x^{N - wt(c)} y^{wt(c)}.$$

Bemerkung 3. *Beachte, dass der Gewichtszähler eines linearen Codes $\mathcal{C} \leq \mathbb{F}_q^N$ ein homogenes Polynom vom Grad N ist. Und es ist*

$$h_\mathcal{C}(x, y) = p_\mathcal{C}(x, y \ldots, y). \tag{1.1}$$

Satz 4 (MacWilliams Identität)**.** *Sei $\mathcal{C} \leq \mathbb{F}_p^N$ ein linearer Code der Länge N und p eine Primzahl. Dann ist*

$$p_{\mathcal{C}^\perp}(x_0, \ldots, x_{p-1}) = \frac{1}{|\mathcal{C}|} p_\mathcal{C}(y_0, \ldots, y_{p-1}),$$

wobei $y_i := \sum_{j=0}^{p-1} \zeta_p^{ij} x_j$ und $\zeta_p = exp(\frac{2\pi i}{p})$ eine primitive p-te Einheitswurzel in $\mathbb{C}$ ist.

Beweis. Wir betrachten die Indikatorfunktion

$$\begin{aligned} \varepsilon : \mathbb{F}_p^N &\longrightarrow \{0,1\} \\ x &\longmapsto \begin{cases} 1, & \text{falls } x \in \mathcal{C}^\perp \\ 0, & \text{sonst} \end{cases} \end{aligned}$$

von $\mathcal{C}^\perp$. Für $v, w \in \mathbb{F}_p^N$ sei

$$\zeta_v(w) := \prod_{i=1}^{N} \zeta_p^{v_i w_i} = \zeta_p^{v \cdot w}.$$

Dann ist für $v \in \mathbb{F}_p^N \cap \mathcal{C}^\perp$

$$v \cdot c = 0 \; \forall c \in \mathcal{C}$$

und somit

$$\sum_{c \in \mathcal{C}} \zeta^{v \cdot c} = \sum_{c \in \mathcal{C}} 1 = |\mathcal{C}|.$$

Andererseits ist für $v \in \mathbb{F}_p^N \cap \mathcal{C}$ die Abbildung $\varphi_v : \mathcal{C} \longrightarrow \mathbb{F}_p, c \mapsto c \cdot v \neq 0$ eine nichttriviale, also eine surjektive lineare Abbildung und daher ist $\mathcal{C} = \dot{\bigcup}_{a \in \mathbb{F}_p} \varphi_v^{-1}(\{a\})$ eine disjunkte Vereinigung gleich großer Mengen. Also ist

$$\sum_{c \in \mathcal{C}} \zeta_p^{v \cdot c} = \frac{|\mathcal{C}|}{p} \sum_{a=0}^{p-1} \zeta_p^a = 0.$$

Mit dieser Überlegung können wir unsere Indikatorfunktion $\varepsilon(v)$ durch

$$\frac{|\mathcal{C}|}{p} \sum_{c \in \mathcal{C}} \zeta_v(c)$$

ersetzen, denn

$$p_{\mathcal{C}^\perp} = \sum_{v \in \mathbb{F}_p^N} \varepsilon(v) \prod_{i=1}^{N} x_{v_i}.$$

Somit erhalten wir folgende Rechnung mit der wir den Beweis vervollständigen

$$\begin{aligned} p_{\mathcal{C}^\perp}(x_0, \ldots, x_{p-1}) &= \sum_{a_1=0}^{p-1} \cdots \sum_{a_N=0}^{p-1} \varepsilon((a_1, \ldots, a_N)) x_{a_1} \ldots x_{a_N} \\ &= \sum_{a_1=0}^{p-1} \cdots \sum_{a_N=0}^{p-1} \frac{1}{\mathcal{C}} \sum_{c \in \mathcal{C}} \prod_{i=1}^{N} \zeta_p^{a_i c_i} x_{a_1} \ldots x_{a_N} \\ &= \frac{1}{\mathcal{C}} \cdot \sum_{c \in \mathcal{C}} \prod_{i=1}^{N} \left(\sum_{j=0}^{p-1} \zeta_p^{j c_i} x_j \right) \\ &= \frac{1}{\mathcal{C}} \cdot p_{\mathcal{C}}(y_0, \ldots, y_{p-1}). \end{aligned}$$

□

Korollar 5. *Der Hamming Gewichtszähler des orthogonalen Codes $\mathcal{C}^\perp$ eines Codes $\mathcal{C} \leq \mathbb{F}_p^N$ ist*

$$h_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|} h_{\mathcal{C}}(x+(p-1)y, x-y).$$

Beweis. Zunächst einmal ist nach (1.1) $h_{\mathcal{C}^\perp}(x,y) = p_{\mathcal{C}^\perp}(x,y\ldots,y)$. Diese Gleichheit formen wir mit Hilfe der MacWilliams Identität (4) zu

$$h_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|} p_{\mathcal{C}}(z_0,\ldots,z_{p-1}),$$

wobei $z_i := x + \sum_{j=1}^{p-1} \zeta_p^{ij} y$ und $\zeta_p = exp(\frac{2\pi i}{p})$ eine primitive p-te Einheitswurzel in $\mathbb{C}$ ist, um. Falls $i = 0$ ist, erhalten wir $z_0 = x+(p-1)y$. Für ein beliebiges $i \in \mathbb{F}_p^*$ und $j = 1,\ldots,p-1$ durchläuft auch ij ganz $\mathbb{F}_p^*$. Daher ist für $i \in \mathbb{F}_p^*$

$$z_i = x + y\sum_{j=1}^{p-1} \zeta_p^{ij} = x + y\sum_{j=1}^{p-1} \zeta_p^{j} = x + y(-1) = x - y.$$

Damit folgt die Behauptung. □

Definition 6. Sei $\mathcal{C} \leq \mathbb{F}_q^N$ ein linearer Code der Länge N.

i) Der Code $\mathcal{C}$ heißt doppelt gerade, falls $wt(c) \in 4\mathbb{Z}\ \forall c \in \mathcal{C}$ ist.

ii) Der Code heißt selbstdual, falls $\mathcal{C} = \mathcal{C}^\perp$ ist.

Bemerkung 7 (Gewichtszähler selbstdualer Codes)**.** *Sei $\mathcal{C} \leq \mathbb{F}_p^N$ ein selbstdualer linearer Code der Länge N mit p prim. So ist $|\mathcal{C}| = p^{N/2}$ und nach (5) ist der Hamming Gewichtszähler von $\mathcal{C}$ gleich*

$$h_{\mathcal{C}}(x,y) = h_{\mathcal{C}^\perp}(x,y) = h_{\mathcal{C}}\left(\frac{x+(p-1)y}{\sqrt{p}}, \frac{x-y}{\sqrt{p}}\right).$$

Damit ist der Hamming Gewichtszähler von $\mathcal{C}$ invariant unter der Variablensubstitution

$$\begin{aligned} x &\mapsto \quad \frac{x+(p-1)y}{\sqrt{p}} \\ y &\mapsto \quad \frac{x-y}{\sqrt{p}} \end{aligned}$$

bzw. als Abbildungsmatrix zur Standardbasis geschrieben

$$\frac{1}{\sqrt{p}} \begin{pmatrix} 1 & p-1 \\ 1 & -1 \end{pmatrix}.$$

Diese Invarianz beschränkt die Menge der möglichen Gewichtszähler selbstdualer Codes. Die möglichen Codes liegen daher alle in dem Teilraum der unter dieser Variablensubstitution invarianten Polynome.

Betrachten wir nun den Spezialfall $p = 2$. Für jedes Codewort c eines selbstdualen Codes $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^N$ ist das Skalarprodukt $c \cdot c = 0$, somit ist die Anzahl der Einsen in $c \in \mathcal{C}$

immer gerade, also $wt(c) \in 2\mathbb{Z}$ *und* $p_{\mathcal{C}}(x_0, x_1) = p_{\mathcal{C}}(x_0, -x_1)$. *Demzufolge ist* $p_{\mathcal{C}}$ *invariant unter der Gruppe von Variablensubstitutionen*

$$\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle =: G_I \cong D_{16}.$$

Für doppelt gerade Codes ist $wt(c) \in 4\mathbb{Z}$, *d.h.* $p_{\mathcal{C}}(x_0, x_1) = p_{\mathcal{C}}(x_0, ix_1)$. *Der Hamming Gewichtszähler eines binären doppelt geraden Codes ist dadurch invariant unter*

$$\langle h := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, d := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \rangle =: G_{II}.$$

G_{II} *ist eine Gruppe der Ordnung 192.*

Korollar 8. *Sei* $\mathcal{C} \leq \mathbb{F}_2^N$ *ein selbstdualer und doppelt gerader linearer Code der Länge* N. *So ist* N *durch* 8 *teilbar.*

Beweis. Wir rechnen leicht nach, dass $(hd)^3 = \zeta_8 I_2 \in G_{II}$ ist. Folglich erfüllt jedes unter G_{II} invariante homogene Polynom p vom Grad N

$$p(x_0, x_1) = p(\zeta_8 x_0, \zeta_8 x_1) = \zeta_8^N p(x_0, x_1).$$

Somit ist $\zeta_8^N = 1$ und infolgedessen ist N durch 8 teilbar. □

Aus der Invariantentheorie sind die folgenden Sätze bekannt (vgl. [5]).

Satz 9. *(I) Ist* $p(x_0, x_1)$ *ein unter* G_I *invariantes Polynom, so ist* p *ein Polynom in* $f := x_0^2 + x_1^2 = p_{\langle (1,1) \rangle}$ *und* $g := x_0^8 + 14x_0^4x_1^4 + x_1^8 = p_{e_8}$ *oder alternativ in* f *und* $\delta_I := \frac{1}{4}(f^4 - g) = x_0^2x_1^2(x_0^2 - x_1^2)^2$.

(II) Ist $p(x_0, x_1)$ *ein unter* G_{II} *invariantes Polynom so ist* p *ein Polynom in* g *und* $\delta_{II} := x_0^4x_1^4(x_0^4 - x_1^4)^4$.

Korollar 10 (Gleason)**.** *Ist* $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^N$, $N = 24a + 8b$ *mit* $0 \leq b \leq 3$ *so gibt es eindeutig bestimmte Zahlen* $k_i \in \mathbb{Z}$, $i = 0, \ldots, a$ *mit* $k_o = 1$ *so, dass*

$$p_{\mathcal{C}}(x_0, x_1) = \sum_{i=0}^{a} k_i f^{4(a-i)+b} \delta_I^i(x_o, x_1).$$

Ist $\mathcal{C}$ *zusätzlich doppelt gerade, so ist* $N = 24a + 8b$ *mit* $0 \leq b \leq 2$ *durch* 8 *teilbar und es gibt eindeutig bestimmte Zahlen* $l_i \in \mathbb{Z}$, $i = 0, \ldots, a$ *mit* $l_0 = 1$ *so, dass*

$$p_{\mathcal{C}}(x_0, x_1) = \sum_{i=0}^{a} l_i g^{3(a-i)+b} \delta_{II}^i(x_o, x_1).$$

Definition 11. Man nennt einen binären doppelt geraden selbstdualen Code $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^N$ mit $N = 24a + 8b$ und $b = 0, 1, 2$ extremal, falls $d(\mathcal{C}) \geq 4a + 4$.

Korollar 12. *Sei* $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^N$ *mit* $N = 24a + 8b$ *ein extremaler Code, dann ist*

$$p_{\mathcal{C}}(1, x) = 1 + A_{4a+4}^* x^{4a+4} + \cdots + A_{4a+4}^* x^{N-4a-4} + x^N$$

eindeutig bestimmt.

Beweis. $p_{\mathcal{C}}(1,x)$ ist eine Linearkombination von $g^{3(a-i)+b}\delta_{II}^{i}(1,x) = x^{4i}(1+\dots)$ für $i = 0,\dots,a$. Also bestimmen die $a+1$ Gleichungen $A_0 = 1$ und $A_d = 0$ für $d = 4,8,\dots,4a$ die Koeffizienten l_i in Gleasons Satz (10) eindeutig. Damit ist $p_{\mathcal{C}}$ eindeutig bestimmt. Weiter gilt $A_d = A_{N-d}$, da die Abbildung $c \mapsto c + \mathbf{1}$ eine Bijektion zwischen den Mengen der Codeworte vom Gewicht d und $N-d$ herstellt. □

Korollar 13. *Ist $\mathcal{C} = \mathcal{C}^{\perp} \leq \mathbb{F}_2^N$ ein doppelt gerader Code, so ist*

$$d(\mathcal{C}) \leq 4\left\lfloor \frac{N}{24} \right\rfloor + 4.$$

Das Korollar (13) wollen wir im folgenden mit endlichen Blockdesigns beweisen, indem wir zeigen, dass die Anzahl A_{4a+4} von Codeworten vom Gewicht $4a+4$ in einem extremalen Code nicht 0 sind.

2 Extremale Codes und Blockdesigns

Definition 14. Seien $v, t, N, k,\ \lambda \in \mathbb{N}$ und $X := \{1, \ldots, N\}$. Das Tupel $(X, \mathcal{D})$ mit der Menge $\mathcal{D} := \{B_1, \ldots, B_v\}$ von k-elementigen Teilmengen $B_i \subset X$, den sogenannten Blöcken, heißt ein t–(N, k, λ) Blockdesign oder Blockplan, falls jede t-elementige Teilmenge T von X in genau λ Blöcken enthalten ist. Man kann auch nur $\mathcal{D}$ als t–(N, k, λ) Blockdesign bezeichnen. Im Falle $\lambda = 1$ sprechen wir von einem Steiner-System.

Satz 15. *Ist $\mathcal{D}$ ein t–(N, k, λ) Blockdesign, so ist die Anzahl der Blöcke*

$$v = |\mathcal{D}| = \lambda \binom{N}{t} / \binom{k}{t} \tag{2.1}$$

Beweis. Sei $\Omega_t := \{T \subset X |\ |T| = t\}$ die Menge aller t–elementigen Teilmengen von X, also $|\Omega_t| = \binom{N}{t}$. Da $\mathcal{D}$ ein t–Design ist, erhalten wir sofort

$$\lambda \binom{N}{t} = \sum_{T \in \Omega_t} |\{B \in \mathcal{D} | T \subset B\}| = \sum_{B \in \mathcal{D}} |\{T \in \Omega_t | T \subset B\}| = |\mathcal{D}| \binom{k}{t}$$

□

Korollar 16. *Ist $\mathcal{D}$ ein Design von unterschiedlicher Stärke, d.h. ein t–(N, k, λ_t) Blockdesign und ein $(t-1)$–(N, k, λ_{t-1}) Blockdesign, dann gilt*

$$\lambda_t (N - t + 1) = \lambda_{t-1} (k - t + 1)$$

Beweis. Nach (2.1) ist

$$\lambda_t \binom{N}{t} / \binom{k}{t} = |\mathcal{D}| = \lambda_{t-1} \binom{N}{t-1} / \binom{k}{t-1}.$$

Dies lässt sich durch einfache elementare Rechnungen zu der obigen Gleichung umformen. □

Bezeichnungen 17. Sei $\mathcal{C} \leq \mathbb{F}_2^N$ ein binärer Code mit $\dim(\mathcal{C}) = k$ und $\mathcal{C}^\perp$ der duale Code. Im Folgenden möchten wir einige Bezeichungen für die nachfolgenden Überlegungen einführen.
Sei $d := d(\mathcal{C})$ und $d' := d(\mathcal{C}^\perp)$. Weiter seien $\mathcal{C}_i$ die Mengen aller Codewörter von $\mathcal{C}$ mit Länge i, d.h. $\mathcal{C}_i = \{c \in \mathcal{C} | wt(c) = i\}$, und $A_i := |\mathcal{C}_i|$. Bezeichne $0 < \tau_1 < \cdots < \tau_s \leq N$ die Gewichte der Codewörter $c \neq 0$ in $\mathcal{C}$ bzw. $\mathcal{C}^\perp$, so ist

$$p_{\mathcal{C}}(1, y) = 1 + \sum_{i=1}^{s} A_{\tau_i} y^{\tau_i}.$$

Beachte, dass es nur ein Wort von Gewicht N, nämlich das Einswort, d.h. $(1, \ldots, 1) \in \mathbb{F}_2^N$, gibt. Dies bedeutet, dass entweder $A_N = 0$ oder $A_N = 1$ ist. Wir bezeichnen außerdem mit $\overline{s}$ die Anzahl der unterschiedlichen Gewichte von Codeworten $c \neq 0$, d.h. $\overline{s} = |\{1 \leq i \leq N-1 | A_i \neq 0\}|$. Im Folgenden wollen wir die Anzahl von Codewörtern mit Hilfe von Blockdesigns, also Teilmengen von $\{1, \ldots, N\}$, bestimmen, daher identifizieren wir die Codewörter von $\mathcal{C}$ mit Elementen von $\mathcal{P}ot(\{1, \ldots, N\})$, indem wir die Worte mit

ihren Trägern identifizieren, z.B. $11001 \in \mathbb{F}_2^5$ entspricht $\{1,2,5\} \in \mathcal{P}ot(\{1,\ldots,5\})$. Mit dieser Identifizierung erkennen wir, dass C_{τ_i} eine Teilmenge von

$$\Omega_{\tau_i} := \{M \subset \{1,\ldots,N| \; |M| = \tau_i\}\}$$

ist.

Lemma 18. *Sei* $\lambda_{\tau_i}(u) := |\{c \in \mathcal{C}_{\tau_i} | u \subset c\}|$. *Dann gilt*

$$\sum_{i=1}^{\overline{s}} \binom{\tau_i - t}{j} \lambda_{\tau_i}(u) = (2^{k-t-j} - A_N)\binom{N-t}{j}$$

für $0 \leq j \leq d' - 1 - t$ *und für* $\forall t$ *mit* $1 \leq t \leq d' - \overline{s}$.

Beweis. (vgl. Nebe, Gitter und Codes, Lemma 7.18) □

Lemma 19. *Sind* $0 < \tau_1 < \cdots < \tau_s \leq N$ *und*

$$T := \begin{pmatrix} 1 & \tau_1 & \binom{\tau_1}{2} & \ldots & \binom{\tau_1}{s} \\ 1 & \tau_2 & \binom{\tau_2}{2} & \ldots & \binom{\tau_2}{s} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \tau_s & \binom{\tau_s}{2} & \ldots & \binom{\tau_s}{s} \end{pmatrix}$$

so ist T *invertierbar mit* $T^{-1} = (f_{ij})$, *wobei*

$$f_i(x) := \prod_{\substack{j=1 \\ j \neq i}}^{s} \frac{\tau_j - x}{\tau_j - \tau_i} = \sum_{j=0}^{s-1} f_{ij} \binom{x}{j}.$$

Beweis.

$$(T \cdot T^{-1})_{i,n} = \sum_{j=0}^{s-1} f_{ij} \binom{\tau_n}{j} = f_i(\tau_n) = \delta_{i,n}.$$

□

Satz 20. *Sei* $1 \leq t \leq d' - \overline{s}$ *und* $\tau_i \geq t \quad \forall i$ *und* $\lambda_{\tau_i}^{(t)} := \lambda_{\tau_i}(1^t, 0^{N-t})$. *Dann ist* C_{τ_i} *ein* t–$(N, \tau_i, \lambda_{\tau_i}^{(t)})$ *Blockdesign.*

Beweis. Je nachdem was $\mathcal{C}$ für ein Code ist, ist $A_N = 0$ oder $A_N = 1$. Nach Lemma (18) erhalten wir also das lineare Gleichungssystem

$$(\lambda_{\tau_1}, \ldots, \lambda_{\tau_{\overline{s}}})T' = (2^{k-t} - A_N, (2^{k-t-1} - A_N)\binom{N-t}{1}, \ldots, (2^{k-d'+1} - A_N)\binom{N-t}{d'-t-1})$$

für die $\lambda_{\tau_i}(u)$ mit der Matrix $T' = \left(\binom{\tau_i - t}{j}\right)_{i,j} \in \mathbb{Z}^{\overline{s} \times d'-1-t}$. Sei $\tilde{\tau_i} := \tau_i - t$, dann ist $0 < \tilde{\tau_1} < \cdots < \tilde{\tau_{\overline{s}}} \leq N$ und somit hat T' nach Lemma (19) Rang $\overline{s}$. Damit lassen sich die $\lambda_{\tau_i}(u)$ mit Hilfe von (19) eindeutig bestimmen. Weiter sind diese unabhängig von $u \in \Omega_t$, also ist C_{τ_i} ein t–$(N, \tau_i, \lambda_{\tau_i}^{(t)})$ Blockdesign. □

Lemma 21. *Sei $1 \leq t \leq d' - \overline{s}$ und $\tau_i \geq t \; \forall i$ und $\lambda_{\tau_i}^{(t)} := \lambda_{\tau_i}(1^t, 0^{N-t})$. Dann ist*

$$\lambda_{\tau_i}^{(t)} S_i(\tau_i) = -A_N S_i(N) + 2^{k-N} \sum_{r=t}^{N} \binom{N-t}{r-t} S_i(r).$$

Beweis. Um die Formel zu beweisen, berechnen wir die λ_{τ_i} aus dem Linearen Gleichungssystem im Beweis von (20) durch lösen der ersten $\overline{s}$ Gleichungen, d.h.

$$(\lambda_{\tau_1}, \ldots, \lambda_{\tau_{\overline{s}}}) = (2^{k-t} - A_N, (2^{k-t-1} - A_N)\binom{N-t}{1}, \ldots, (2^{k-t-\overline{s}+1} - A_N)\binom{N-t}{\overline{s}-1})\tilde{T}^{-1}$$

mit $\tilde{T} = \left(\binom{\tau_i - t}{j}\right)_{i,j} \in \mathbb{Z}^{\overline{s} \times \overline{s}}$ und $\tilde{T}^{-1} = \tilde{f_{ij}}$, wobei

$$\tilde{f}_i(x) = f_i(x+t) = \prod_{\substack{j=1 \\ j \neq i}}^{\overline{s}} \frac{\tau_j - t - x}{\tau_j - \tau_i} = \sum_{j=0}^{\overline{s}-1} \tilde{f_{ij}} \binom{x}{j} = \sum_{j=0}^{\overline{s}-1} f_{ij} \binom{x+t}{j}.$$

Somit ist

$$\begin{aligned}
\lambda_{\tau_i} &= \sum_{j=0}^{\overline{s}-1} (2^{k-t-j} - A_N) \binom{N-t}{j} \tilde{f_{ij}} \\
&= 2^{k-N} \sum_{j=0}^{\overline{s}-1} (2^{N-t-j} - 2^{N-k} A_N) \binom{N-t}{j} \tilde{f_{ij}} \\
&= 2^{k-N} \left(\sum_{j=0}^{\overline{s}-1} (2^{N-t-j} \binom{N-t}{j} \tilde{f_{ij}} - \sum_{j=0}^{\overline{s}-1} 2^{N-k} A_N) \binom{N-t}{j} \tilde{f_{ij}} \right)
\end{aligned}$$

Für die erste Summe ist

$$\begin{aligned}
2^{N-t-j} \binom{N-t}{j} &= \sum_{n=0}^{N-t-j} \binom{N-t-j}{n} \binom{N-t}{j} \\
&= \sum_{n=j}^{N-t} \binom{N-t-j}{n-j} \binom{N-t}{j} \\
&= \sum_{n=j}^{N-t} \binom{N-t}{n} \binom{n}{j},
\end{aligned}$$

da $\binom{M-j}{n-j}\binom{M}{j} = \binom{M}{n}\binom{n}{j}$ ist.

Somit können wir das Ganze zu

$$\begin{aligned}
\lambda_{\tau_i} &= 2^{k-N} \sum_{m=0}^{N} \binom{N-t}{m} \sum_{j=0}^{\overline{s}-1} \tilde{f_{ij}} \binom{m}{j} - A_N \sum_{j=0}^{\overline{s}-1} \tilde{f_{ij}} \binom{N-t}{j} \\
&= 2^{k-N} \sum_{m=0}^{N-t} \binom{N-t}{m} \tilde{f}_i(m) - A_N \tilde{f}_i(N-t) \\
&= 2^{k-N} \sum_{m=t}^{N} \binom{N-t}{m-t} \tilde{f}_i(m-t) - A_N f_i(N-t+t) \\
&= 2^{k-N} \sum_{m=t}^{N} \binom{N-t}{m-t} f_i(m) - A_N f_i(N)
\end{aligned}$$

vereinfachen. Mit $S_i(x)$ aus den Voraussetzungen ergibt sich

$$\frac{S_i(x)}{S_i(\tau_i)} = \left(\prod_{\substack{j=1\\ j\neq i}}^{\overline{s}}(\tau_i - x)\right)\cdot\left(\prod_{\substack{j=1\\ j\neq i}}^{\overline{s}}(\tau_j - \tau_i)\right)^{-1} = \prod_{\substack{j=1\\ j\neq i}}^{\overline{s}}\frac{(\tau_i - x)}{(\tau_j - \tau_i)} = f_i(x).$$

Also ist

$$\lambda_{\tau_i}S_i(\tau_i) = -A_N S_i(N) + 2^{k-N}\sum_{m=t}^{N}\binom{N-t}{m-t}S_i(m).$$

□

Korollar 22. *Sei $1 \leq t \leq d' - \overline{s}$ und $\tau_i \geq t\ \forall i$ und $\lambda_{\tau_i}^{(t)} := \lambda_{\tau_i}(1^t, 0^{N-t})$. Dann ist*

$$A_N S(N) = 2^{k-N}\sum_{r=t-1}^{N}\binom{N-t+1}{r-t+1}S(r)$$

für $2 \leq t \leq d' - \overline{s}$.

Beweis. Nach (20) ist C_{τ_i} ein t- und ein $(t-1)$-Blockdesign. Und somit ist nach Korollar (16)

$$\lambda_{\tau_i}^{(t)}(N-t+1) = \lambda_{\tau_i}^{(t-1)}(\tau_i - t + 1). \tag{2.2}$$

Damit ergibt sich durch einsetzen von $\lambda_{\tau_i}^{(t)}$ und $\lambda_{\tau_i}^{(t-1)}$ aus Lemma (21)

$$\begin{aligned} & \frac{(N-t+1)A_N S(N)}{N-\tau_i} + (N-t+1)2^{k-N}\sum_{r=t}^{N}\binom{N-t}{r-t}\frac{S(r)}{(\tau_i - r)} \\ = \quad & \frac{(\tau_i - t+1)A_N S(N)}{(N-\tau_i)} + (\tau_i - t+1)2^{k-N}\sum_{r=t-1}^{N}\binom{N-t+1}{r-t+1}\frac{S(r)}{(\tau_i - r)}. \end{aligned}$$

Diese Rechnung ist aber auch äquivalent zu der folgenden Überlegung

$$\begin{aligned} & \frac{A_N S(N)(N-t+1)}{(N-\tau_i)} - \frac{A_N S(N)(\tau_i - t+1)}{(N-\tau_i)} \\ = \quad & (\tau_i - t+1)2^{k-N}\sum_{r=t-1}^{N}\binom{N-t+1}{r-t+1}\frac{S(r)}{(\tau_i - r)} - (N-t+1)2^{k-N}\sum_{r=t}^{N}\binom{N-t}{r-t}\frac{S(r)}{(\tau_i - r)} \end{aligned}$$

bzw. zu

$$\begin{aligned} & A_N S(N)\left[\frac{(N-t+1)}{(N-\tau_i)} - \frac{(\tau_i - t+1)}{(N-\tau_i)}\right] \\ = \quad & 2^{k_N}[(\tau_i - t+1)\sum_{r=t-1}^{N}\binom{N-t+1}{r-t+1}\frac{S(r)}{(\tau_i - r)} - \sum_{r=t}^{N}\binom{N-t}{r-t}\frac{S(r)}{(\tau_i - r)}]. \end{aligned}$$

Weiter rechnen wir leicht nach, dass

$$\binom{N-t}{r-t}(N-t+1) = (r-t+1)\binom{N-t+1}{r-t+1}$$

ist und somit lässt sich das Ganze zu

$$A_N S(N) = 2^{k-N}[(\tau_i - t + 1) \sum_{r=t-1}^{N} \binom{N-t+1}{r-t+1} \frac{S(r)}{(\tau_i - r)} - \sum_{r=t}^{N} \binom{N-t+1}{r-t+1} \frac{(r-t+1)S(r)}{(\tau_i - r)}]$$

vereinfachen. Da aber auch

$$\binom{N-t+1}{t-1-t+1} = \binom{N-t+1}{0} = 0$$

ist, erhalten wir insgesamt

$$A_N S(N) = 2^{k-N}[\sum_{r=t-1}^{N} \binom{N-t+1}{r-t+1} S(r) \frac{\tau_i - t + 1 - r + t - 1}{(\tau_i - r)}].$$

□

Satz 23. *Sei $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^N$ ein doppelt gerader Code der Länge $N = 24a + 8b$ mit $d(\mathcal{C}) \geq 4a + 4$. Dann ist $d(\mathcal{C}) = 4a + 4$ und für die Anzahl A^*_{4a+4} von Codewörtern von Gewicht $4a + 4$ gilt*

$$\begin{aligned}
A^*_{4a+4} &= \binom{N}{5}\binom{5a-2}{a-1}\binom{4a+4}{5} && \text{falls } N = 24a \\
A^*_{4a+4} &= \frac{1}{4}N(N-1)(N-2)(N-4)\frac{(5a)!}{a!(4a+4)!} && \text{falls } N = 24a+8 \\
A^*_{4a+4} &= \frac{3}{2}N(N-2)\frac{(5a+2)!}{a!(4a+4)!} && \text{falls } N = 24a+16.
\end{aligned}$$

Weiter ist $\mathcal{C}_{4a+4}$ ein $(5-2b)$–Design.

Beweis. Es ist $d = d'$ und

$$\begin{aligned}
\overline{s} &= |\{4a+4, 4a+8, \ldots, N-(4a+4) = 20a-4+8b\}| \\
&= \frac{20a-4+8b}{4} - \frac{4a+4-4}{4} = 4a-1+2b.
\end{aligned}$$

Demnach ist C_{τ_i} nach Satz (20) ein Blockdesign der Stärke

$$d' - \overline{s} = 4a + 4 - (4a - 1 + 2b) = 5 - 2b.$$

Wir wollen im Folgenden nur die Formel für $N = 24a$ beweisen. Da $\mathcal{C}$ ein binärer doppelt gerader Code ist, ist $A_N = 1$ und Lemma (21) liefert

$$\lambda^{(t)}_{\tau_i} S_i(\tau_i) = -S_i(N) + 2^{k-N} \sum_{r=t}^{N} \binom{N-t}{r-t} S_i(r).$$

Wir betrachten nun $\tau_i := 4a + 4$ und erhalten

$$\begin{aligned}
S_i(\tau_i) &= (4a+8-(4a+4)) \cdot (4a+12-(4a+4)) \cdot \cdots \cdot (20a-4-(4a+4)) \\
&= 4 \cdot 8 \cdot \cdots \cdot (16a-8) \\
&= 4^{4a-2}(4a-2)!
\end{aligned}$$

als auch

$$\begin{aligned} S_i(N) &= (4a+8-24a)\cdot\cdots\cdot(20a-4-24a) \\ &= (-20a+8)\cdot\cdots\cdot(-4a-4) \\ &= (-1)^{4a-2}(20a-8)\cdot\cdots\cdot(4a+4) \\ &= 4(a+1)\cdot\cdots\cdot 4(5a-2) \\ &= 4^{4a-2}\tfrac{(5a-2)!}{a!}. \end{aligned}$$

Somit ist für $t=4$ und $\tau_i = 4a+4$

$$\lambda^{(4)}_{4a+4}4^{4a-2}(4a-2)! = -4^{4a-2}\frac{(5a-2)!}{a!} + 2^{12a-24a}\cdot\sum_{r=4}^{2} 4a\binom{24a-4}{r-4}\frac{S(r)}{4a+4-r} \quad (2.3)$$

wobei $S(r) = \prod_{i=1}^{4a-1}(4a+4i-r)$ ist. Nun gelten die nachfolgenden Gleichheiten:

- $\dfrac{S(r-4)-S(r)}{16a-4} = \dfrac{S(r)}{4a+4-r}$
- $\displaystyle\sum_{r=4}^{24a}\binom{24a-4}{r-4}S(r-4) = -\sum_{l=4}^{24a}\binom{24a-4}{l-4}S(l)$
- $\dfrac{1}{2^{12a}}\displaystyle\sum_{r=4}^{24a}\binom{24a-4}{r-4}S(r) = S(24a) = -4^{4a-1}\dfrac{(5a-1)!}{a!}.$

Die erste Gleichung erhalten wir aus

$$S(r-4) = S(r)\frac{20a-r}{4a+4-r} = S(r) + \frac{(20a-r)-(4a+4-r)}{4a+4-r}S(r),$$

also

$$\frac{S(r-4)-S(r)}{16a-4} = \frac{((20a-r)-(4a+4-r))S(r)}{(4a+4-r)(16a-4)}.$$

Um die zweite Gleichung zu beweisen betrachten wir

$$\begin{aligned} S(24a-r) &= \prod_{i=1}^{4a-1}(4a+4i-(24a-r)) \\ &= \prod_{i=1}^{4a-1}(-20a+4i+r) \\ &= (-20a+4+r)\cdot(-20a+8+r)\cdot\cdots\cdot(-20a+16a-4+r) \\ &= (-1)^{4a-1}(20a-4-r)\cdot(20a-8-r)\cdot\cdots\cdot(4a+4-r) \\ &= -S(r). \end{aligned}$$

Damit ist

$$\begin{aligned} -\sum_{l=4}^{24a}\binom{24a-4}{l-4}S(l) &= \sum_{l=4}^{24a}\binom{24a-4}{24a-l}S(24a-l) \\ &= \sum_{r=0}^{24a-4}\binom{24a-4}{r}S(r) \\ &= \sum_{r=4}^{24a}\binom{24a-4}{r-4}S(r-4). \end{aligned}$$

Nach Korollar (22) ist C_{4a+4} ein 4– als auch ein 5–Blockdesign. Da $A_N = 1$ ist, erhalten wir mit (22) das erste Gleich in der dritten Gleichung. Das letzte Gleich erhalten wir aus

$$\begin{aligned} S(24a) &= S_i(24a) \cdot (\tau_i - 24a) \\ &= S_i(24a) \cdot (4a + a - 24a) \\ &= 4^{4a-2}\frac{(5a-2)!}{a!}(-20a+4) \\ &= 4^{4a-2}\frac{(5a-2)!}{a!}(-4)(5a-1) \\ &= -4^{4a-1}\frac{(5a-1)!}{a!} \end{aligned}$$

Demnach lässt sich der zweite Summand von (2.3) zu

$$\begin{aligned} 2^{-12a}\sum_{r=4}^{24a}\binom{24a-4}{r-4}\frac{S(r)}{4a+4-r} &= 2^{-12a}\sum_{r=4}^{24a}\binom{24a-4}{r-4}\frac{S(r-4)-S(r)}{16a-4} \\ &= -2^{-12a}\tfrac{1}{8a-2}\sum_{r=4}^{24a}\binom{24a-4}{r-4}S(r) \\ &= -\frac{S(24a)}{8a-2} \\ &= 4^{4a-1}\frac{(5a-1)!}{a!(8a-2)} \end{aligned}$$

vereinfachen und daher ist

$$\lambda^{(4)}_{4a+4}4^{4a-2}(4a-2)! = -4^{4a-2}\frac{(5a-2)!}{a!} + 4^{4a-1}\frac{(5a-1)!}{a!(8a-2)}$$

bzw.

$$\lambda^{(4)}_{4a+4} = \frac{(6a-1)(5a-2)!}{a!(4a-1)!}.$$

Mit diesem Wert ergibt sich

$$\begin{aligned} \lambda^{(5)}_{4a+4} &= |\mathcal{D}|\binom{4a+4}{5}/\binom{24a}{5} \\ &= \lambda^{(4)}_{4a+4}\binom{24a}{4}/\binom{4a+4}{4}\cdot\binom{4a+4}{5}/\binom{24a}{5} \\ &= \lambda^{(4)}_{4a+4}\frac{4a}{24a-4} \\ &= \binom{5a-2}{a-1} \end{aligned}$$

und somit ist die Anzahl von Worten vom Gewicht $4a+4$ gleich

$$\lambda^{(4)}_{4a+4}\binom{24a}{5}/\binom{4a+4}{5}.$$

□

Satz 24. *Sei $\mathcal{C} \leq \mathbb{F}_2^N$ ein binärer doppelt gerader selbstdualer Code der Länge $N = 24a$ und $d(\mathcal{C}) = 4a + 4$. Dann bildet $\mathcal{C}_{\tau_i}$ ein t–$(N, \tau_i, \lambda_{\tau_i}^{(t)})$ Blockdesign für $1 \leq t \leq 5$ und*

$$\lambda_{4a+8}^{(4)} = \frac{6a-1}{a}\binom{5a-2}{a-1}\left(\binom{20a-4}{4}/\binom{4a+4}{4} - (4a-1)\right) + \binom{5a-1}{a+1} - \binom{5a-3}{a-1}.$$

Insbesondere ist $A_{4a+8}^* < 0$ für $a \geq 154$, d.h. ein solcher Code kann höchstens eine Länge von maximal $24 \cdot 153 = 3672$ haben. (s. [3])

Dieser Satz zeigt, dass es nur endlich viele extremale Codes der Länge $N = 24a$ gibt. Analoge Resultate erhält man auch für $N = 24a + 8b$, $b = 1, 2$.

Satz 25. *Die Anzahl der extremalen Codes ist endlich.*

Definition 26. Ein Code $\mathcal{C} \leq \mathbb{F}_q^N$ heißt perfekt, falls es eine Zahl t gibt, so dass zu jedem $a \in \mathbb{F}_q^N$ genau ein $c \in \mathcal{C}$ existiert mit $d(a, c) := wt(a - c) \leq t$.

Satz 27. *Ein Code $\mathcal{C} \leq \mathbb{F}_q^N$ ist genau dann perfekt, wenn $2^N = |\mathcal{C}| \cdot \sum_{i=0}^{t} \binom{N}{i}$ gilt.*

Satz 28. *Sei $\mathcal{C} \leq \mathbb{F}_2^{24}$, $dim(\mathcal{C}) = 12$ und $d(\mathcal{C}) = 8$. Dann ist $\mathcal{C}$ ein extremaler doppeltgerader selbstdualer Code. Weiter gibt es bis auf Äquivalenz höchstens einen solchen Code $\mathcal{C}$.*

Beweis. Sei $\mathcal{C}'$ der Code der Länge 23, der aus $\mathcal{C}$ entsteht, indem man eine Spalte aus $\mathcal{C}$ weglässt. Dann ist $|\mathcal{C}'| = 2^{12}$, da sich aufgrund des Minimalabstandes von $\mathcal{C}$ verschiedene Codeworte an mindestens 8 Stellen unterscheiden müssen. Insbesondere ist somit der Minimalabstand von $\mathcal{C}'$ gleich 7. Weiter sind die Hamming-Kugeln

$$B_3(c) := \{x \in \mathbb{F}_2^N | d(x, c) \leq 3\}$$

mit Radius 3 um die Codeworte von $\mathcal{C}'$ disjunkt. Da

$$2^{12}(1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}) = 2^{23}$$

ist, ist $\mathcal{C}'$ nach Satz (27) ein perfekter Code. Wir definieren uns zunächst einmal

$$X_j := \{(x, c') \in \mathbb{F}_2^N \times \mathcal{C}' | w(x) = j, d(x, c') \leq 3\}$$

für $j = 1, \ldots, 23$. Nun berechnen wir die Mächtigkeit von X_j auf zwei verschiedene Weisen und kommen somit an unsere A_i. Da $\mathcal{C}'$ ein perfekter Code ist, existiert für jedes $x \in \mathbb{F}_2^{23}$ genau ein $c' \in \mathcal{C}'$ mit $wt(x - c') \leq 3$. Somit ist $|X_j| = |\{x \in \mathbb{F}_2^N | wt(x) = j\}| = \binom{23}{j}$. Andererseits ist

$$|X_j| = \sum_{i=0}^{23} A_i \cdot |\{x \in \mathbb{F}_2^N | wt(x) = j, wt(x - \tilde{c}_i) \leq 3, \tilde{c}_i \in \mathcal{C}', wt(\tilde{c}_i) = i\}|.$$

Man beachte, dass $|\{x \in \mathbb{F}_2^N | wt(x) = j, wt(x - \tilde{c}_i) \leq 3, \tilde{c}_i \in \mathcal{C}', wt(\tilde{c}_i) = i\}| \neq 0$, falls $j - 3 \leq i \leq j + 3$ ist und sonst gleich 0. Mit dieser Überlegung erhalten wir die Rekursionsgleichung

$$\begin{aligned}
\binom{23}{j} = & \quad A_{j+3} \cdot \binom{j+3}{j} + A_{j+2} \cdot \binom{j+2}{j} \\
+ & \quad A_{j+1} \cdot \left(\binom{j+1}{j} + \binom{j+1}{j-1}\binom{23-j-1}{1} \right) \\
+ & \quad A_j \cdot \left(\binom{j}{j} + \binom{j}{j-1}\binom{23-j}{1} \right) \\
+ & \quad A_{j-1} \cdot \left(\binom{23-(j-1)}{1} + \binom{j-1}{j-2}\binom{23-(j-1)}{2} \right) \\
+ & \quad A_{j-2} \cdot \binom{23-(j-2)}{2} + A_{j-3} \cdot \binom{23-(j-3)}{3}
\end{aligned} \tag{2.4}$$

Da wir wissen, dass $A_0 = 1$ und $A_1 = A_2 = \ldots A_6 = 0$ ist, lassen sich die Anzahlen rekursiv berechnen:

$$\begin{array}{rcrcr}
A'_0 & = & A'_{23} & = & 1 \\
A'_7 & = & A'_{16} & = & 253 \\
A'_{11} & = & A'_{12} & = & 1288 \\
A'_8 & = & A'_{15} & = & 506.
\end{array}$$

Diese sind unabhängig davon, welche Stelle von $\{1, \ldots, 24\}$ gestrichen worden ist. Also sind die Gewichte von $\mathcal{C}'$ immer $\equiv_4 -1, 0$ und daher ist $wt(\mathcal{C}) \subset 4\mathbb{Z}$, denn sei:

Fall 1: $wt(\mathcal{C}) \equiv_4 2$ dann wäre $wt(\mathcal{C}') \equiv_4 1$ oder 2. Also ein Widerspruch.

Fall 2: $wt(\mathcal{C}) \equiv_4 3$ dann wäre $wt(\mathcal{C}') \equiv_4 2$ oder -1. Was im ersten Fall einen Widerspruch bedeutet.

Fall 3: $wt(\mathcal{C}) \equiv_4 1$ dann wäre $wt(\mathcal{C}') \equiv_4 1$ oder 0. Was im ersten Fall einen Widerspruch bedeutet.

Somit ist

$$p_{\mathcal{C}}(1, y) = 1 + 759y^8 + 2576y^{12} + 759y^{16} + y^{24}$$

und $\mathcal{C}$ doppelt gerade. Insbesonder ist $\mathcal{C} \subset \mathcal{C}^\perp$ bzw. $\mathcal{C} = \mathcal{C}^\perp$ aus Dimensionsgründen. Sei nun $u \in \mathcal{C}$ vom Gewicht 12 und $\mathcal{C}_u$ der Code, der aus $\mathcal{C}$ entsteht, indem alle Spalten von $\mathcal{C}$ gestrichen werden, in denen $u_i = 1$ ist. Wir bezeichnen mit π_u die Abbildung dieses Streichens. Dann ist $\mathcal{C}_u = Bild(\pi_u)$ und $Kern(\pi_u) = \{u, 0\}$. Also ist $\mathcal{C}_u$ gerade, hat Länge 12 und Dimension 11, da $\dim(Kern(\pi_u)) = 1$ ist. Somit ist $\mathcal{C}_u$ der gerade Teilcode von $\mathbb{F}_2^{12}$ und durch geeignete Umordnung der Spalten hat $\mathcal{C}$ eine Erzeugermatrix der Form

$$\mathcal{G} := \left(\begin{array}{c|c|c|c} 1^{11} & 1 & 0 & 0^{11} \\ \hline A & 0_{11} & 1_{11} & I_{11} \end{array} \right)$$

mit $1^{11} := (1, \ldots, 1) \in \{0,1\}^{1\times 11}$,
$0^{11} := (0, \ldots, 0) \in \{0,1\}^{1\times 11}$,
$1_{11} := (1, \ldots, 1)^\perp \in \{0,1\}^{11\times 1}$,
$0_{11} := (0, \ldots, 0)^\perp \in \{0,1\}^{11\times 1}$,

I_{11} die Einheitsmatrix und $A \in \mathbb{F}_2^{11\times 11}$, wobei jede Zeile in A mindestens Gewicht 6 hat und je zwei Zeilen von A einen Abstand von mindestens 6 haben. Da aber jede Zeile von $\mathcal{G}$ mindestens einen Abstand von 8 zu der ersten Zeile, d.h. zu u, haben muss, hat jede Zeile von A ein Gewicht von 6. Daher sieht man auch, dass je zwei Zeilen von A genau Abstand 6 haben, da die Summe von zwei Zeilen von A ebenfalls Gewicht 6 haben muss. Somit haben zwei Zeilen von A genau zwei Nullen gemeinsam. Umgekehrt können wir schließen, dass es für zwei beliebige Positionen –$\binom{11}{2}$ Möglichkeiten– der Nullen genau ein Paar von Zeilen –$\binom{11}{2}$ Möglichkeiten– gibt, die dort das gemeinsame Paar von Nullen haben. Denn angenommen es gäbe drei Zeilen von A, die dort das gemeinsame Paar von Nullen besitzen, so hätte A o.B.d.A. Zeilen der Form

$$\begin{array}{cccccccccccc} & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ \hline \oplus & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

Die dritte Zeile erhalten wir aus den Voraussetzungen, dass die letzten beiden Positionen 0 sind und der Abstand zwischen den Zeilen immer 6 ist. Addieren wir nun die entsprechenden Zeilen in $\mathcal{G}$ so erhalten wir das Wort

$$c = (0^{11} |\ 1\ |\ 1\ |\ 0 \ldots 0\ 1\ 0 \ldots 0\ 1\ 0 \ldots 0) \in \mathbb{F}_2^{24}$$

Das Wort c hat Gewicht 4 und ist somit $\notin \mathcal{C}$, ein Widerspruch zur Annahme. Also ist A die Inzidensmatrix eines 2–$(11, 5, 2)$ Blockdesigns, das eindeutig bestimmt ist. □

Im abschließenden Abschnitt werden wir nun einen binären extremalen, doppeltgeraden und selbstdualen Code der Länge 24 mit Hilfe von Steinersystemen konstruieren.

3 Der erweiterte binäre Golay-Code

Satz 29. *Sei $G = PSL(2, 23)$ und $X = \mathbb{Z}_{23} \cup \{\infty\}$. Dann ist $W_{24} = (X, G \cdot B)$ mit $B = \{\infty, 0, 1, 3, 12, 15, 21, 22\}$ ein 5–$(24, 8, 1)$ Steiner-System. Dabei ist G die projektive spezielle lineare Gruppe über dem Körper $\mathbb{F}_{23}$ und ist folgendermaßen definiert*

$$PSL(n, q) := SL(n, q)/\{\lambda \cdot I_n | \lambda^n = 1\}.$$

Man kann die Abbildungen aus $PSL(2, q)$ auch als Abbildung

$$x \mapsto \frac{ax + b}{cx + d} \text{ mit } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL(2, q)$$

darstellen. Ein Element ist genau dann aus der $PSL(2, q)$, wenn $ad - bc$ ein Quadrat in $\mathbb{F}_q$ ist.

Beweis. Die Abbildungen

$$\alpha : x \mapsto \frac{x + 1}{-x + 1} \text{ und } \beta : x \mapsto \frac{3x + 1}{x - 3}$$

sind in der $PSL(2, 23)$, denn:

$$1 \cdot 1 - (1 \cdot (-1)) = 2 = 5^2 \text{ und } 3 \cdot (-3) - 1 \cdot 1 = -10 = 6^2.$$

Desweiteren rechnet man leicht nach, dass die Abbildungen die Gleichungen

$$\alpha^4 = \beta^2 = \text{id}$$
$$\beta\alpha\beta = \alpha^{-1}$$

erfüllen. Daher erzeugen α und β eine Untergruppe U von $PSL(2, 23)$ von der Ordnung 8 (s. Diedergruppen $|D_4| = 8$).

$$U = \{id, \alpha, \beta, -\frac{1}{x}, \frac{x - 1}{x + 1}, \frac{x + 2}{2x - 1}, \frac{-2x + 1}{x + 2}, \frac{-x + 3}{3x + 1}\}$$

Wir definieren nun B als

$$B := U \cdot \infty = \{\infty, 0, 1, 3, 12, 15, 21, 22\}$$

(hierbei nutzt man, dass $\frac{a \cdot \infty + b}{c \cdot \infty + d} =: \frac{a}{c}$ für $c \neq 0$, $\frac{a \cdot \infty + b}{c \cdot \infty + d} =: \infty$ für $a \neq 0, c = 0$ und $\frac{e}{0} =: \infty$ für $e \neq 0$). Mit diesem B gilt: $U \cdot B = B$, was leicht zu zeigen ist. Daher wissen wir nun, dass $|G_B|$ ein Vielfaches von 8 sein muss, d.h. $|G_B| = 8 \cdot m$, $m \in \mathbb{N}$. Hiermit folgern wir, dass die Zahl $b = |G \cdot B|$ der Blöcke gleich

$$\frac{|G|}{|G_B|} = \frac{2^3 \cdot 3 \cdot 11 \cdot 23}{2^3 \cdot m} = \frac{759}{m}$$

ist und dass die Zahl der Blöcke die ∞, 0 und 1 enthalten

$$\lambda_3 = b \cdot \frac{8 \cdot 7 \cdot 6}{24 \cdot 23 \cdot 22} = \frac{21}{m}$$

ist ($\lambda_3 = b \cdot \binom{8}{3} / \binom{24}{3}$). Betrachte nun die Abbildungen

$$\sigma + 1 : x \mapsto 1 - \frac{1}{x} = \frac{x-1}{x+0}.$$

Diese Abbildung fixiert $\{0, 1, \infty\}$ und permutiert die Menge $\{a, b, c, d, e\}$ mit $\{\infty, 0, 1, a, b, c, d, e\} \in G \cdot B$. Durch mehrfache Anwendung von $\sigma + 1$ auf die Mengen $\{a, b, c, d, e\}$ von

$B = \{\infty, 0, 1, 3, 12, 15, 21, 22\}$	$2B = \{\infty, 0, 1, 2, 6, 7, 19, 21\}$
$2B - 6 = \{\infty, 0, 1, 13, 15, 17, 18, 19\}$	$8B - 7 = \{\infty, 0, 1, 8, 16, 17, 20, 21\}$
$B + 2 = \{\infty, 0, 1, 2, 3, 5, 14, 17\}$	$2B - 1 = \{\infty, 0, 1, 5, 6, 18, 20, 2\}$
$8B - 4 = \{\infty, 0, 1, 3, 4, 11, 19, 20\}$	

erhalten wir alle 21 möglichen Mengen $\{a, b, c, d, e\}$; daher $m = 1$. Die Mengen sind die Spalten der 21×5 Matrix:

$$\left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc}
3 & 16 & 11 & 2 & 12 & 22 & 2 & 12 & 22 & 5 & 10 & 17 & 13 & 8 & 21 & 3 & 16 & 11 & 8 & 21 & 13 \\
12 & 22 & 2 & 3 & 16 & 11 & 6 & 20 & 9 & 6 & 20 & 9 & 15 & 4 & 18 & 4 & 18 & 15 & 16 & 11 & 3 \\
15 & 4 & 18 & 5 & 10 & 17 & 7 & 14 & 19 & 18 & 15 & 4 & 17 & 5 & 10 & 11 & 3 & 16 & 17 & 5 & 10 \\
21 & 13 & 8 & 14 & 19 & 7 & 19 & 7 & 14 & 20 & 9 & 6 & 18 & 15 & 4 & 19 & 7 & 14 & 20 & 9 & 6 \\
22 & 2 & 12 & 17 & 5 & 10 & 21 & 13 & 8 & 22 & 2 & 12 & 19 & 7 & 14 & 20 & 9 & 6 & 21 & 13 & 8
\end{array}\right)$$

Die 21 Spalten formen ein 2–$(21, 5, 1)$ auf der Punktmenge $V \backslash \{\infty, 0, 1\}$. Der Beweis dazu ist einfach, aber sehr mühsam. Damit ist $(X, G \cdot B)$ ein $S(5, 8; 24)$ Steiner-System, da G dreifach transitiv auf X operiert. □

Lemma 30. *Sei $\mathcal{D} = (X, \mathcal{B})$ ein 5–$(24, 8, 1)$ Steiner-System und U eine Teilmenge eines Blocks B in $\mathcal{D}$. Dann ist die Zahl $n(B, U)$ der Blöcke C in $\mathcal{D}$ mit $B \cap C = U$ nur vom Parameter $u = |U|$ abhängig, d.h. $n(B, U) = n_u$, und hat folgende Werte*

$$n_8 = 1, n_7 = n_5 = n_3 = n_1 = 0, n_4 = 4, n_2 = 16, n_0 = 30$$

Insbesondere ist $|B \cap B'|$ gerade für je zwei Blöcke B und B'.

Beweis. Sei $U \subset X$ eine u-Teilmenge, wobei $u \leq 5$. U ist in genau $\binom{24-u}{5-u}$ 5 - Teilmengen T von X enthalten, und jede hiervon in genau einem Block. Von den U umfassenden Blöcken wird aber so jeder genau $\binom{8-u}{5-u}$-fach gezählt, denn er enthält so viele 5-elementige Mengen, die U umfassen. Also ist die Anzahl der U umfassenden Blöcke gleich $\binom{24-u}{5-u} / \binom{8-u}{5-u}$ und insbesondere unabhängig von U.
Damit folgt: $\lambda_5 = 1, \lambda_4 = 5, \lambda_3 = 21, \lambda_2 = 77, \lambda_1 = 253, \lambda_0 = 759$
$\lambda_u =$ Anzahl der U enthaltenden Blöcke mit $u = |U|$.
Wir definieren nun die Mengen

$$\mathcal{B}_u := \{C \in \mathcal{B} : U \subset C\},$$

also $|\mathcal{B}_u| = \lambda_u$ und

$$\mathcal{B}_{u,r} := \{C \in \mathcal{B}_u : |B \cap C| = \mathrm{r}\},$$

also ist $|\mathcal{B}_{u,r}| = \mathrm{n_u}$.
Offenbar ist $\mathcal{B}_{u,8} = \{\mathrm{B}\}$ und $\mathcal{B}_{u,r} = \emptyset$ für $r \in \{5,6,7\}$, denn 5 oder mehr Punkte bestimmen eindeutig den Block B. Also ist $\mathrm{n_8} = 1, \mathrm{n_7} = \mathrm{n_6} = \mathrm{n_5} = 0$.
Sei nun u = 4. Wegen dem ersten Teil des Beweises wissen wir, dass es $5 = \lambda_4$ Blöcke C gibt, die U enthalten. Für dieses C gilt $B \cap C = U$ außer für $C = B$. Also ist $\mathrm{n}_u = \mathrm{n_4} = 5 - 1 = 4$. Sei nun u = 3. Offensichtlich ist

$$\mathcal{B}_u = \mathcal{B}_{u,3} \,\dot\cup\, \mathcal{B}_{u,4} \,\dot\cup\, \mathcal{B}_{u,8}$$

mit $\mathcal{B}_{u,8} = \{\mathrm{B}\}$. $\mathcal{B}_{u,4}$ zerfällt in $5 = 8 - 3$ Teilmengen jeweils zum vierten Punkt $x \in \mathrm{B}$ mit $\mathrm{B} \cap \mathrm{C} = \mathrm{U} \cup \{x\}$ mit $\mathrm{C} \in \mathcal{B}_{u,4}$.
Damit ist $\lambda_3 = \mathrm{n_3} + (8-3)\mathrm{n_4} + 1$ und somit $\mathrm{n}_u = \mathrm{n_3} = 0$.
Entsprechen d erhält man für u = 2

$$\mathcal{B}_u = \mathcal{B}_{u,2} \,\dot\cup\, \mathcal{B}_{u,3} \,\dot\cup\, \mathcal{B}_{u,4} \,\dot\cup\, \mathcal{B}_{u,8}$$

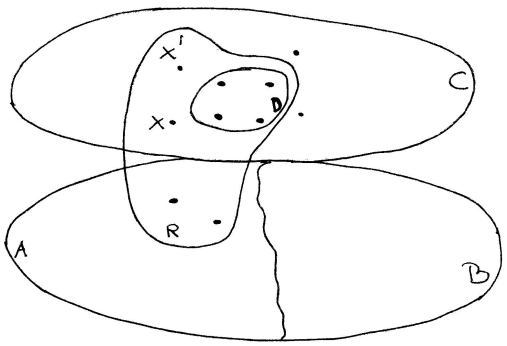
also $\lambda_2 = \mathrm{n}_u + (8-2)\mathrm{n_3} + \binom{8-2}{2}\mathrm{n_4} + 1$ und damit haben wir $\mathrm{n_2} = 4$
und für u = 1 bzw. u = 0 erhält man

$$\lambda_1 = \mathrm{n_1} + (8-1)\mathrm{n_2} + \binom{8-1}{2}\mathrm{n_3} + \binom{8-1}{3}\mathrm{n_4} + 1$$
$$\text{bzw. } \lambda_0 = \mathrm{n_0} + 8\mathrm{n_1} + \binom{8}{2}\mathrm{n_2} + \binom{8}{3}\mathrm{n_3} + \binom{8}{4}\mathrm{n_4} + 1$$

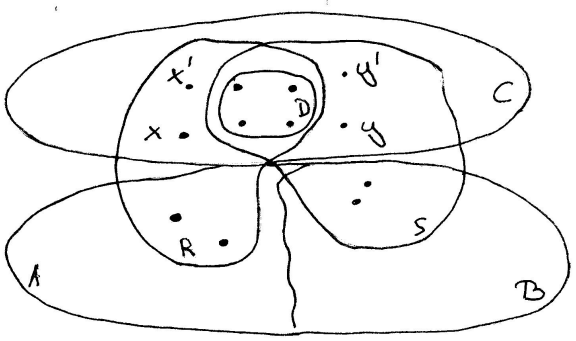
also $\mathrm{n_1} = 0$ und $\mathrm{n_0} = 30$. □

Lemma 31. *Sei $\mathcal{D} = (X, \mathcal{B})$ ein 5–$(24, 8, 1)$ Steiner-System, A und B zwei disjunkte Blöcke in $\mathcal{D}$, dann ist auch $C = X \backslash (A \cup B)$ ein Block in $\mathcal{D}$.*

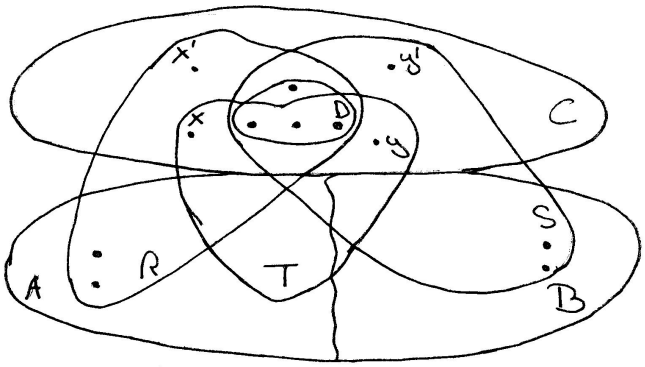
Beweis. Wähle eine 4-elementige Teilmenge D von C und einen Punkt $x \in C \backslash D$. Sei R der durch $D \cup \{x\}$ bestimmte Block. Sei $R \neq C$ so ist $A \cap R \neq \emptyset$ oder $B \cap R \neq \emptyset$. Wegen (30) schneidet R entweder A oder B in zwei Punkten, denn es existiert kein Block, der mit R genau einen oder genau drei Punkte gemeinsam hat, o.B.d.A. ist $|R \cap A| = 2$ und $R \cap B = \emptyset$, d.h. es existiert ein eindeutiges $x' \in C \backslash (D \cup \{x\})$.



Seien y und y' die beiden übrigen Punkte von C. Weiter bezeichne $S \neq C$ den Block der durch $D \cup \{y\}$ eindeutig definiert ist. Da $y \notin R$ ist $R \neq S$ und wegen (30) ist $|S \cap B| = 2$ (argumentiere wie oben, $S \cap A = \emptyset$, da $R \neq S$).



Betrachte nun jeden Block T, der durch 3 belieige Punkte von D, durch x und y festgelegt ist.



Wegen (30) schneidet T entweder A oder B in zwei Punkten, also muss T C in einem weiteren Punkt schneiden, also entweder in x', y' oder dem vierten Punkt von D, d.h. T schneidet R oder S in 5 Punkten. Damit folgt $T = R$ oder $T = S$, aber andererseits ist $y \notin T$ und $x \notin S$. Damit erhalten wir einen Widerspruch. □

Lemma 32. *Sei $\mathcal{D} = (X, \mathcal{B})$ ein 5–$(24, 8, 1)$ Steiner-System. Je zwei Blöcke A und B aus $\mathcal{D}$ mit $|A \cap B| = 2$ bilden als symmetrische Differenz $D = A \triangle B = (A \cup B) \backslash (A \cap B)$ eine 12-elementige Teilmenge, welche Dodekad in $\mathcal{D}$ genannt wird. Es gibt höchstens 132 Block-Paare (Y, Z) mit $D = Y \triangle Z$. Im Falle von Gleichheit, bildet die Klasse ξ_D aller Blöcke von $\mathcal{D}$ die D in genau 6 Punkten schneiden ein 5–$(12, 6, 1)$ Steiner-System in D.*

Beweis. Je 5 Punkte von D legen einen Block Y in $\mathcal{D}$ eindeutig fest. Offenbar ist die maximale Zahl von Partitionen $D = Y \triangle Z$ festgelegt, falls jeder Block Y, der durch 5 Punkte festgelegt ist, genau 6 Punkte von D enthält, so dass $Z = D \triangle Y$ auch ein Block ist. In diesem Fall gibt es $\binom{12}{5} / \binom{6}{5} = 132$ solcher Partitionen $D = Y \triangle Z$, mit der trivialen Konsequenz, dass ξ_D ein $S(5, 6; 12)$ formt. □

Satz 33. *Sei $\mathcal{D} = (X, \mathcal{B})$ ein 5–$(24, 8, 1)$ Steiner-System und $\mathcal{C} \subset \{0,1\}^X$ sei der von $\mathcal{B}$ erzeugte Vektorraum. Dann hat $\mathcal{C}$ die Dimension 12 und besteht aus*

i) $\emptyset, X$

ii) 759 Blöcken und deren Komplemente

iii) 2576 Dodekaden

Der Vektorraum $\mathcal{C}$ wird als erweiterter binärer Golay-Code bezeichnet. Dieser ist ein extremaler doppeltgerader selbstdualer binärer Code der Länge 24.

Beweis. Offenbar enthält $\mathcal{C}$ die 759 Blöcke (s. Beweis von (29)) von $\mathcal{B}$. Wähle nun zwei disjunkte Blöcke A und B. Wegen (31) ist $C = X \backslash (A \cup B)$ ein weiterer Block, welcher disjunkt zu A und B ist, d.h. ein Punkt aus X ist in genau einem der drei Blöcke enthalten. Damit wissen wir, dass ein Punkt aus X in genau $\frac{759}{3} = 253$ Blöcken liegt. Somit ist die Summe aller 759 Blöcke genau X. Folglich enthält $\mathcal{C}$ X und insbesondere die Komplemente der Blöcke als auch $\emptyset$.
Nun seien A und B beliebige Blöcke, die als Vektoren betrachtet werden. Dann gilt mit dem Standard-Skalarprodukt

$$A \cdot B = \sum_{i=1}^{24} a_i b_i = |A \cap B| \bmod 2.$$

Wegen (30) ist $|A \cap B| \bmod 2 = 0$ für alle Blöcke A, B und daher gilt:

$$Y \cdot Z = 0 \qquad \forall\, Y, Z \in \mathcal{C},$$

was $\mathcal{C} \subset \mathcal{C}^\perp$ impliziert, also $\dim \mathcal{C} \leq 12$.
Es genügt nun zu zeigen, dass es mindestens 2576 Dodekade gibt, denn es gilt:

$$2 + 2 \cdot 759 + 2576 = 4096 = 2^{12} = |\{0,1\}^X|.$$

Da es wegen Satz (30) $759 \cdot 16 \cdot \binom{8}{2}$ Blockpaare (A, B) gibt mit $|A \cap B| = 2$ folgt mit (32), dass es mindestens $\frac{759 \cdot 16 \cdot \binom{8}{2}}{132} = 2576$ Dodekade in $\mathcal{C}$ gibt, also folgt insbesondere mit der obigen Gleichung, dass es genau 2576 Dodekade gibt. □

Literatur

[1] Beth, Thomas und Dieter Jungnickel: *Mathieu Groups, Witt Designs, And Golay Codes*. Lecture Notes in Mathematics: Geometries and Groups, (893):157–179, 1981.

[2] Beth, Thomas, Dieter Jungnickel und Hanfried Lenz: *Design Theory. Vol 1.* Cambridge: University Press., 1999.

[3] MacWilliams, F.J. und N.J.A. Sloane: *The Theory of Error-Correcting Codes*, Band 16. north-holland publishing company, Amsterdam, New York, Oxford, 1977.

[4] Nebe, Prof. Dr. Gabriele: *Gitter und Codes, Skript.* 2007.

[5] Sturmfels, Bernd: *Algorithms in Invariant Theory.* Springer Verlag, Wien, New York, 1993.