Gewichtszähler von Codes

Vortrag zum Seminar Gitter und Codes, 11.05.2015

Ronas Karakas

In diesem Vortrag wird der Gewichtszähler von Codes eingeführt und es werden Anwendungen auf Modulformen und Theta-Funktionen gegeben. Zudem werden mit der MacWilliams-Identität sowie dem Satz von Gleason zwei zentrale Aussagen zu diesem Thema bewiesen, welche in der Theorie binärer linearer Codes von großer Bedeutung sind. Des Weiteren beinhaltet der Vortrag Anwendungen und Folgerungen dieser beiden Sätze sowie Einführung in extremale Codes. Die Grundlage dieses Vortrages bildet [1].

§1 Hilfsaussagen

Zunächst halten wir einige Aussagen aus früheren Vorträgen fest, welche im Vortrag ihre Verwendung finden werden. Die Beweise lassen sich in den Ausarbeitungen von den vorherigen Vorträgen finden.

Zur Erinnerung folgende

(1.1) Definition

(i) Ein Code C der Länge $n \in \mathbb{N}$ ist eine Teilmenge von $\mathbb{F}_q^n$. Im Fall $q = 2$ nennt man ihn Binärcode.

(ii) Für $x \in \mathbb{F}_q^n$ heißt $w(x) := |\{i \in \underline{n} \mid x_i \neq 0\}|$ das Gewicht von x. Für $x, y \in \mathbb{F}_q^n$ ist $d(x,y) := w(x-y)$ der Abstand von x und y.

(iii) Ein Code C heißt linear, falls C ein Untervektorraum von $\mathbb{F}_q^n$ ist. Ist $k := dim(C)$ und $d := min\{d(x,y) | x, y \in C\}$, so nennt man C einen $[n,k,d]$ Code.

(iv) Es gilt: $C^\perp = \{y \in \mathbb{F}_q^n \mid \Phi(x,y) = 0 \text{ für alle } x \in C\}$ ◇

Weitere Eigenschaften von Codes charakterisieren wir in der folgenden

(1.2) Definition

(i) Ein linearer Code C heißt selbstdual, falls $C = C^\perp$.

(ii) Ein Binärcode C heißt doppelt gerade, falls $w(x) \in 4\mathbb{Z}$ gilt für alle $x \in C$. ◇

Eine wichtige Verbindung von Binärcodes und Gittern findet sich in folgendem

(1.3) Lemma

(i) Sei C ein $[n,k,d]$ Binärcode. Wir definieren die Reduktionsabbildung mod 2: $\rho : \mathbb{Z}^n \to \mathbb{F}_2^n, x \mapsto [x]_2$ sowie $\Gamma_C := \frac{1}{\sqrt{2}}\rho^{-1}(C)$. Dann ist Γ_C ein Gitter in $\mathbb{R}^n$.

(ii) Es gilt $\det(\Gamma_C) = 2^{n-2k}$

(iii) C ist doppelt gerade genau dann, wenn Γ_C ein gerades Gitter ist.

(iv) C ist selbstdual genau dann, wenn Γ_C ein unimodulares Gitter ist.

(v) Es gilt die Identität $\Gamma_C^{\#} = \Gamma_{C^\perp}$. ◇

Eine weitere wichtige Funktion beinhaltet folgende

(1.4) Bemerkung

Sei $\Gamma \subseteq \mathbb{R}^n$ ein Gitter. Für $x, y \in \Gamma$ bezeichne $\Phi(x,y)$ das Standardskalarprodukt von x und y.

(i) Für $\tau \in \mathbb{H}$ definieren wir $q := e^{2\pi i\tau}$. Dann heißt $\vartheta_\Gamma(\tau) := \sum_{x\in\Gamma} q^{\frac{1}{2}\Phi(x,x)}$ die Theta-Funktion von Γ.

(ii) Sei nun Γ ein gerades Gitter. Für $\tau \in \mathbb{H}$ gilt dann $\vartheta_\Gamma(\tau) = \sum_{r=0}^{\infty} a_r q^r$, wobei $a_r := |\{x \in \Gamma \mid \Phi(x,x) = 2r\}|$. ◇

Es folgt eine weitere wichtige

(1.5) Definition

Sei $k \in \mathbb{Z}$. Eine holomorphe Funktion $f : \mathbb{H} \to \mathbb{C}$ heißt Modulform vom Gewicht k, falls folgende Bedingungen erfüllt sind:

(i)

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau) \text{ für alle } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

(ii) f hat eine Fourier-Reihenentwicklung in $q := e^{2\pi i\tau}$, die bei $n = 0$ anfängt, d.h. f ist holomorph in $i\infty$. ◇

Eine zentrale Aussage beinhaltet der folgende

(1.6) Satz

Sei Γ ein gerades unimodulares Gitter in $\mathbb{R}^n$. Dann gilt:

(i) $n \equiv 0 \pmod 8$.

(ii) ϑ_Γ ist eine Modulform vom Gewicht $\frac{n}{2}$. ◇

Als Nächstes erinnern wir uns noch an folgenden

(1.7) Satz

(i) Die Algebra der Modulformen M ist isomorph zu $\mathbb{C}[E_4, E_6]$, in Zeichen: $M \cong \mathbb{C}[E_4, E_6]$.

(ii) Es gilt $M_{12}^0 \cong M_0 \cong \mathbb{C}$, genauer ist der Isomorphismus gegeben durch Multiplikation mit $\Delta := \frac{1}{1728}(E_4^3 - E_6^2)$. ◇

Zuletzt erwähnen wir folgendes

(1.8) Lemma (Transformationsformel für Theta-Reihen)
Für ein Gitter $\Gamma \subset \mathbb{R}^n$ sowie $\tau \in \mathbb{H}$ gilt:

$$\vartheta_\Gamma(-\frac{1}{\tau}) = (\frac{\tau}{i})^{\frac{n}{2}} \cdot \frac{1}{\mathrm{vol}(\mathbb{R}^n/\Gamma)} \vartheta_{\Gamma^\#}(\tau)$$

§ 2 Der Gewichtszähler von Codes

In diesem Abschnitt wird, wie aus der Überschrift bereits deutlich wird, der Gewichtszähler von Codes eingeführt und es werden erste Anwendungen und Beispiele gegeben.

Wir kommen nun zur zentralen

(2.1) Definition
Sei $C \subseteq \mathbb{F}_q^n$ ein Code der Länge n. Dann ist der Hamming-Gewichtszähler von C definiert als das Polynom

$$W_C(X, Y) := \sum_{u \in C} X^{n-w(u)} Y^{w(u)}.$$ ◇

Erste Eigenschaften halten wir fest in folgendem

(2.2) Lemma

(i) Es gilt: $W_C(X, Y) = \sum_{i=0}^n A_i X^{n-i} Y^i$, wobei $A_i := |\{u \in C \mid w(u) = i\}|$

(ii) Es gilt: $W_C(X, Y) \in \mathbb{F}_q[X, Y]_{hom,n} := \{p \in \mathbb{F}_q[X, Y] \mid f \text{ homogen, } \mathrm{grad}(p) = n\}$.

(iii) Sei nun C ein $[n,k,d]$ Code. Dann gilt:

$$\sum_{i=0}^{n} A_i = q^k.$$

◇

Beweis

(i) Per Definition ist $w(u) \in \{0,\dots,n\}$ für alle $u \in C$. Damit haben wir also, dass $X^{n-w(u)}Y^{w(u)} = X^{n-i}Y^i$ für jedes $u \in C$ ist, wobei $i \in \{0,\dots n\}$ ist. Für $i \in \{0,\dots,n\}$ taucht das Monom $X^{n-i}Y^i$ per Definition genau A_i mal auf. Damit folgt die Aussage.

(ii) Das folgt aus der Definition, da man nur Monome vom Grad n aufsummiert.

(iii) Es gilt:

$$\sum_{i=0}^{n} A_i \overset{\text{Def. } A_i}{=} |\{u \in C \mid w(u) \in \{0,\cdots n\}\}| \overset{\text{Def. } w(u)}{=} |C| = q^k$$

□

Zum Aufwärmen folgt ein erstes

(2.3) Beispiel

(i) Wir betrachten den Hamming-Code $H \subseteq \mathbb{F}_2^7$. Nach dem Vortrag über Codes und Codegitter gilt $A_0 = A_7 = 1, A_3 = A_4 = 7$ und $A_1 = A_2 = A_5 = A_6 = 0$. Damit folgt:

$$W_H(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7.$$

(ii) Nun betrachten wir den erweiterten Hamming-Code $\tilde{H} \subseteq \mathbb{F}_2^8$. Hier gilt analog, dass $A_0 = A_8 = 1, A_4 = 14$ und $A_i = 0$ für alle $i \in \{1,2,3,5,6,7\}$. Damit folgt:

$$W_{\tilde{H}}(X,Y) = X^8 + 14X^4Y^4 + Y^8.$$

◇

Als nächstes behandeln wir eine wichtige Aussage in folgendem

(2.4) Lemma

Sei $C \subset \mathbb{F}_2^n$ ein selbstdualer, doppelt gerader Binärcode. Dann gilt $n \equiv 0 \pmod 8$. ◇

Beweis

Wir betrachten das zugehörige Gitter Γ_C definiert wie in (1.3). Nach (1.3) ist Γ_C dann ein gerades, unimodulares Gitter in $\mathbb{R}^n$. Mit Satz (1.6) folgt dann $n \equiv 0 \pmod 8$. □

Es folgt eine Identität für die Koeffizienten der Fourier-Reihe von speziellen Modulformen.

(2.5) Lemma
Sei f eine Modulform mit Gewicht 12 und

$$f(\tau) = \sum_{r=0}^{\infty} a_r q^r$$

die Fourier-Reihenentwicklung in q. Dann gilt:

$$a_2 = -24a_1 + 196560a_0. \qquad \diamond$$

Beweis
Nach (1.7)(i) ist die Algebra der Modulformen isomorph zu $\mathbb{C}[E_4, E_6]$. Da die Linearkombinationen von E_4^3 und E_6^2 die einzigen Modulformen mit Gewicht 12 sind und man diese auch durch $\Delta := \frac{1}{1728}(E_4^3 - E_6^2)$ und E_6^2 erhält, reicht es, die Identität für diese beiden nachzurechnen.

Aus dem Vortrag über Eisensteinreihen ist uns bereits bekannt:

$$\Delta = 0 \cdot 1 + q - 24q^2 + \text{ Terme höherer Ordnung}$$

sowie

$$E_6 = 1 - 504q - 504 \cdot 33q^2 + \text{ Terme höherer Ordnung.}$$

Mit dem Cauchy-Produkt für Reihen folgt dann für die Koeffizienten von E_6^2:

$$E_6^2 = 1 - 504q - 504q + 504^2q^2 - 504 \cdot 33q^2 - 504 \cdot 33q^2 + \sum_{r=3}^{\infty} c_r q^r$$

$$= 1 - 1008q + 220752q^2 + \sum_{r=3}^{\infty} c_r q^r, \text{ wobei } c_r \in \mathbb{Z}$$

Nun gilt aber:

$$-24 = -24 \cdot 1 + 196560 \cdot 0$$

und

$$220752 = -24 \cdot (-1008) + 196560 \cdot 1.$$

Somit folgt die Behauptung. $\square$

Hieraus erhält man direkt die

(2.6) Folgerung
Sei $\Gamma \subseteq \mathbb{R}^{24}$ ein gerades unimodulares Gitter. Dann gilt für die Theta-Funktion ϑ_Γ:

$$a_2 = 196560 - 24a_1. \qquad \diamond$$

Beweis
Nach Satz (1.6) ist ϑ_Γ eine Modulform von Gewicht 12. Zudem folgt mit (1.4)(ii), dass $a_0 = 1$ ist. Wir wenden (2.5) an und erhalten insgesamt:

$$a_2 = 196560 - 24a_1. \qquad \square$$

Nun folgt eine Aussage über die Gewichtsverteilung spezieller Binärcodes.

(2.7) Lemma
Sei C ein selbstdualer, doppelt gerader Binärcode der Länge 24. Für $i \in \underline{24}$ sei A_i so definiert wie in (2.2)(i). Dann gilt:

(i) $A_i = 0$ für alle $i \in \underline{24}$ mit $i \not\equiv 0 \pmod 4$

(ii) $A_8 = 759 - 4A_4$. $\diamond$

Beweis

(i) Da C doppelt gerade ist, gilt $w(x) \in 4\mathbb{Z}$ für alle $x \in C$. Damit folgt:

$$A_i := |\{u \in C \mid w(u) = i\}| = 0, \text{ falls } i \not\equiv 0 \pmod 4.$$

(ii) Sei $\vartheta_C := \vartheta_{\Gamma_C}$ die Theta-Funktion vom Gitter Γ_C. Wegen (1.4) ist dann für $\tau \in \mathbb{H}$:

$$\vartheta_C(\tau) = \sum_{r=0}^{\infty} a_r q^r.$$

Dabei gilt:

$$a_1 := |\{x \in \Gamma_C \mid \Phi(x,x) = 2\}| \text{ und } a_2 := |\{x \in \Gamma_C \mid \Phi(x,x) = 4\}|$$

Zeige nun:

$$(1)\ a_1 = 24 \cdot 2 + 16A_4.$$

Für $c \in C$ sei $\tilde{c}$ die Identifikation in $\{0,1\}^{24} \subset \mathbb{Z}^{24}$, indem man die Restklassen auf die entsprechende Zahl aus $\{0,1\}$ abbildet. Sei nun $x \in \Gamma_C$. Dann gilt $x = \frac{1}{\sqrt{2}}(\tilde{c} + 2y)$ mit $y \in \mathbb{Z}^{24}$. Damit $\Phi(x,x) = 2$ ist, muss nun gelten:

$$\Phi(x,x) = \frac{1}{2}(\Phi(\tilde{c},\tilde{c}) + 4\Phi(\tilde{c},y) + 4\Phi(y,y)) = 2, \text{ d.h.}$$

$$2\Phi(x,x) = \Phi(\tilde{c},\tilde{c}) + 4\Phi(\tilde{c},y) + 4\Phi(y,y) = 4. \qquad \circledast$$

Für das zu $\tilde{c}$ gehörige $c \in C$ betrachten wir nun folgende Fälle:

1. Falls $w(c) = 4$ ist, folgt auch $\Phi(\tilde{c}, \tilde{c}) = 4$, da $\tilde{c} \in \{0,1\}^{24}$ dann 4 Einsen und sonst nur Nullen als Eintrag hat.

Falls nun $\Phi(\tilde{c}, y) = 0$ ist, muss wegen $\circledast$ bereits $\Phi(y, y) = 0$, d.h. $y = 0$ gelten. Falls jedoch $\Phi(\tilde{c}, y) \neq 0$ gilt, folgt wegen $\Phi(\tilde{c}, \tilde{c}) = 4$, $\Phi(y, y) \geq 0$ und $\circledast$, dass $\Phi(\tilde{c}, y) < 0$ gelten muss. Wegen $\tilde{c} \in \{0,1\}^{24}$ sind die Einträge von y an den Stellen, an denen $\tilde{c}_i \neq 0$ gilt, nicht-positiv. Zudem ist $y_i = 0$ für alle $i \in \underline{24}$ mit $\tilde{c}_i = 0$, denn angenommen, es gibt ein $i \in \underline{24}$ mit $y_i \neq 0$. und $\tilde{c}_i = 0$. Dann wäre $|\tilde{c}_i + 2y_i| \geq 2$. Da y_i 4 Nichtnulleinträge hat, würde gelten:

$$\frac{1}{2}\Phi(\tilde{c} + 2y, \tilde{c} + 2y) > \frac{4}{2} = 2.$$

Das kann aber wiederum nicht sein. Weiterhin gilt $y_i \in \{-1, 0\}$ für alle $i \in \underline{24}$, denn angenommen, es gibt ein $i \in \underline{24}$ mit $y_i \leq -2$. Dann wäre $\tilde{c}_i + 2y_i \leq -3$. Damit würde aber gelten:

$$\frac{1}{2}\Phi(\tilde{c} + 2y, \tilde{c} + 2y) \geq \frac{9}{2} > 2,$$

was ein Widerspruch dazu wäre, dass $\Phi(x, x) = 2$ ist.

Da $\tilde{c}$ 4 Nichtnulleinträge hat und $y \in \{-1, 0\}^{24}$, erhalten wir aus dem oben Gezeigten somit $2^4 = 16$ Möglichkeiten für y. In diesen ist $y = 0$ auch enthalten. Somit ist insgesamt gezeigt, dass jedes $c \in A_4$ genau 16 Möglichkeiten für x liefert, sodass $\Phi(x, x) = 2$ ist. Somit erhalten wir aus diesem Fall insgesamt $16 \cdot A_4$ Möglichkeiten für x.

2. Nun betrachten wir als nächstes den Fall $w(c) = 0$. Dann ist $\tilde{c} = 0$. Da $\Phi(x, x) = \frac{1}{2}\Phi(\tilde{c} + 2y, \tilde{c} + 2y) = 2\Phi(y, y) = 2$ gelten muss und $y \in \mathbb{Z}^{24}$, folgt:

$$y_i \in \{-1, 1\} \text{ für ein } i \in \underline{24} \text{ und } y_j = 0 \text{ für alle } j \in \underline{24} \setminus \{i\}.$$

Damit erhalten wir in diesem Fall also insgesamt $2 \cdot 24$ Möglichkeiten.

3. Falls nun $w(c) \notin \{0, 4\}$ ist, folgt $w(c) \in \{8, 12, 16, 20, 24\}$, da $C \subset \mathbb{Z}^{24}$ doppelt gerade ist. Für beliebiges $y \in \mathbb{Z}^{24}$ hat $\tilde{c} + 2y \in \mathbb{Z}^{24}$ mindestens 8 Nichtnulleinträge. Dann würde aber gelten:

$$\Phi(x, x) = \frac{1}{2}\Phi(\tilde{c} + 2y, \tilde{c} + 2y) \geq \frac{8}{2} > 2.$$

Damit würde x nicht mehr die gewünschte Eigenschaft erfüllen, somit tritt der 3. Fall nie auf.

Insgesamt haben wir also gezeigt:

$$a_1 = 24 \cdot 2 + 16A_4.$$

Somit ist (1) bewiesen. Als nächstes zeigen wir:

$$(2)\ a_2 = 2^8 \cdot A_8 + 16A_4 \cdot 20 \cdot 2 + \binom{24}{2} \cdot 4.$$

Hierfür geht man genauso vor wie bei (1) und folgert:

Für $w(c) = 8$ erhalten wir (vergleiche den 1. Fall bei (1)) 2^8 Möglichkeiten.
Für $w(c) = 4$ erhalten wir genau $16 \cdot 20 \cdot 2$ Möglichkeiten, da y die Form wie beim 1. Fall aus (1) hat, wobei noch zusätzlich ein weiterer der 20 restlichen Einträge 1 oder -1 ist. Die Argumentation vergleichbar mit Fall 1. aus (1).
Für $w(c) = 0$ erhalten wir $\binom{24}{2} \cdot 4$ Möglichkeiten, weil y dann genau zwei Nichtnulleinträge hat, welche dann 1 oder -1 sein müssen.
Die restlichen Fälle treten nicht auf, da mit analoger Ausführung wie bei (1) folgen würde, dass $\Phi(x, x)$ zu groß wäre.

Da Γ_C nach (1.3) ein gerades, unimodulares Gitter ist, wenden wir nun (2.6) an und erhalten:

$$2^8 \cdot A_8 + 16A_4 \cdot 20 \cdot 2 + \binom{24}{2} \cdot 4 = a_2 = 196560 - 24a_1 = 196560 - 24(24 \cdot 2 + 16A_4).$$

Durch Umformen erhalten wir

$$A_8 = \frac{194304 - 1024A_4}{2^8} = 759 - 4A_4.$$ □

Als nächstes beweisen wir eine weitere Eigenschaft des Gewichtszählers.

(2.8) Lemma
Für einen linearen Code $C \subset \mathbb{F}_q^n$ und $k \in \mathbb{N}$ definieren wir $C^k := \bigoplus_{i=1}^k C$. Dann gilt:

$$W_{C^k}(X, Y) = (W_C(X, Y))^k.$$ ◇

Beweis
Nach Definition der direkten Summe ist $C^k \subset \mathbb{F}_q^{nk}$. Damit folgt:

$$W_{C^k}(X, Y) = \sum_{u \in C^k} X^{nk - w(u)} Y^{w(u)} = \sum_{u_1, \ldots, u_k \in C} X^{nk - w(u_1, \ldots, u_k)} Y^{w(u_1, \ldots, u_k)}$$

$$= \sum_{u_1, \ldots, u_k \in C} X^{nk - \sum_{j=1}^k w(u_j)} Y^{\sum_{j=1}^k w(u_j)} = (\sum_{u \in C} X^{n - w(u)} Y^{w(u)})^k = W_C(X, Y)^k.$$ □

Zur Veranschaulichung betrachten wir ein

(2.9) Beispiel
Sei $C := \tilde{H} \oplus \tilde{H} \oplus \tilde{H} \subset \mathbb{F}_2^{24}$. Dann ist C doppelt gerade, da $\tilde{H}$ es ist und wir die dreifache direkte Summe von $\tilde{H}$ mit sich selbst betrachten. Zudem ist C selbstdual, denn C ist 12 dimensional, da $\tilde{H}$ vierdimensional ist. Da zudem $\tilde{H}$ selbstdual ist, gilt $C \subset C^{\perp}$, womit aus Dimensionsgründen die Gleichheit folgt. Nun folgt:

$$W_C(X,Y) \overset{(2.8)}{=} (W_{\tilde{H}}(X,Y))^3 = X^{24} + 42X^{20}Y^4 + 591X^{16}Y^8 + \sum_{i=12}^{24} A_i X^{24-i}Y^i.$$

Weiterhin gilt:

$$591 = 759 - 168 = 759 - 4 \cdot 42.$$ ◇

Durch die Aussagen aus (2.6) und (2.7) kommt man auf folgende Fragestellungen:
1. Gibt es ein gerades unimodulares Gitter der Dimension 24, für dessen Theta-Funktion gilt: $a_1 = 0$? Dazu lässt sich sagen, dass dieses nicht von der Form Γ_C mit C wie in (2.7) sein kann, da wir im Beweis gesehen haben, dass $a_1 \geq 48$ ist.
2. Existiert ein linearer Code $C \subset \mathbb{F}_2^{24}$ mit $A_4 = 0$? Falls es solch einen gibt, weiß man wegen (2.7) bereits, dass er genau 759 mit Gewicht 8 haben muss. Wir beenden den Abschnitt mit folgender

(2.10) Bemerkung
Das Leech-Gitter erfüllt die in 1. gesuchten Eigenschaften. Der in 2. gesuchte Code ist durch den erweiterten Golay Code $\tilde{G}$ eindeutig bestimmt. ◇

Dies wird im Vortrag von Herrn Pawelzik ausgeführt.

§ 3 Die MacWilliams-Identität und der Satz von Gleason

In diesem Abschnitt werden, wie aus dem Namen bereits deutlich wird, diese beiden, bedeutenden Sätze eingeführt und bewiesen. Weiterhin werden Anwendungen und Beispiele dieser gegeben.

Zunächst führen wir zwei Funktionen ein, die wir in diesem Abschnitt des Öfteren betrachten werden.

(3.1) Definition
Für $\tau \in \mathbb{H}$ definieren wir

(i)

$$A(\tau) := \sum_{x \in \mathbb{Z}} q^{\Phi(x,x)} = \sum_{x \in \mathbb{Z}} q^{x^2} \text{ sowie}$$

(ii)

$$B(\tau) := \sum_{x \in 2\mathbb{Z}+1} q^{\frac{1}{4}\Phi(x,x)} = \sum_{x \in 2\mathbb{Z}+1} q^{\frac{1}{4}x^2}.$$

◇

Nun stellen wir erste, elementare Eigenschaften dieser Funktionen vor.

(3.2) Lemma
(i) Sei $\Gamma = \sqrt{2}\mathbb{Z}$. Dann gilt: $A = \vartheta_\Gamma$.

(ii) B ist nicht die Theta-Funktion eines Gitters.

(iii) Es gelten für alle $\tau \in \mathbb{H}$ die folgenden Identitäten:

(a)

$$A\left(-\frac{1}{\tau}\right) = \left(\frac{\tau}{i}\right)^{1/2} \frac{1}{\sqrt{2}}(A(\tau) + B(\tau)),$$

(b)

$$B\left(-\frac{1}{\tau}\right) = \left(\frac{\tau}{i}\right)^{1/2} \frac{1}{\sqrt{2}}(A(\tau) - B(\tau)).$$

◇

Beweis
(i) Für $\tau \in \mathbb{H}$ gilt:

$$\vartheta_\Gamma(\tau) = \sum_{x \in \sqrt{2}\mathbb{Z}} q^{\frac{1}{2}\Phi(x,x)} = \sum_{x \in \mathbb{Z}} q^{\frac{1}{2}\Phi(\sqrt{2}\cdot x, \sqrt{2}\cdot x)} = \sum_{x \in \mathbb{Z}} q^{\Phi(x,x)} = A(\tau).$$

(ii) Für ein beliebiges Gitter gilt $a_0 = 1$, jedoch folgt aus der Definition von B, dass kein konstanter Term auftaucht. Damit folgt die Aussage.

(iii) Zu (a): Für $\tau \in \mathbb{H}$ gilt:

$$A(\tau)+B(\tau)=\sum_{x\in\sqrt{2}\mathbb{Z}} q^{\frac{1}{2}\Phi(x,x)}+\sum_{x\in 2\mathbb{Z}+1} q^{\frac{1}{4}\Phi(x,x)}=\sum_{x\in 2\mathbb{Z}} q^{\frac{1}{4}\Phi(x,x)}+\sum_{x\in 2\mathbb{Z}+1} q^{\frac{1}{4}\Phi(x,x)}$$
$$=\sum_{x\in\mathbb{Z}} q^{\frac{1}{4}\Phi(x,x)}=\sum_{x\in\frac{1}{\sqrt{2}}\mathbb{Z}} q^{\frac{1}{2}\Phi(x,x)}=\vartheta_{\frac{1}{\sqrt{2}}\mathbb{Z}}(\tau)$$

Zudem ist $\frac{1}{\sqrt{2}}\mathbb{Z}$ das duale Gitter zu $\sqrt{2}\mathbb{Z}$. Wir wenden (1.8) an und erhalten:

$$A\left(-\frac{1}{\tau}\right)=\left(\frac{\tau}{i}\right)^{1/2}\cdot\frac{1}{\mathrm{vol}(\mathbb{R}/\sqrt{2}\mathbb{Z})}\cdot\vartheta_{\frac{1}{\sqrt{2}}\mathbb{Z}}(\tau)$$
$$=\left(\frac{\tau}{i}\right)^{1/2}\cdot\frac{1}{\sqrt{\det(\sqrt{2}\mathbb{Z})}}(A(\tau)+B(\tau))=\left(\frac{\tau}{i}\right)^{1/2}\cdot\frac{1}{\sqrt{2}}(A(\tau)+B(\tau)).$$

Zu (b): Wir setzen in die Formel von (a) den Wert $-\frac{1}{\tau}\in\mathbb{H}$ ein und erhalten:

$$A(\tau)=\left(-\frac{1}{\tau i}\right)^{1/2}\cdot\frac{1}{\sqrt{2}}\left(A\left(-\frac{1}{\tau}\right)+B\left(-\frac{1}{\tau}\right)\right).$$

Durch erneutes Einsetzen von (a) erhalten wir:

$$A(\tau)=\left(-\frac{1}{\tau i}\right)^{1/2}\cdot\frac{1}{\sqrt{2}}\left(\left(\frac{\tau}{i}\right)^{1/2}\cdot\frac{1}{\sqrt{2}}(A(\tau)+B(\tau))+B\left(-\frac{1}{\tau}\right)\right).$$

Durch Umformen erhält man:

$$A(\tau)-B(\tau)=\left(-\frac{1}{\tau i}\right)^{1/2}\cdot\sqrt{2}B\left(-\frac{1}{\tau}\right)$$

und schließlich

$$B\left(-\frac{1}{\tau}\right)=\left(\frac{\tau}{i}\right)^{1/2}\frac{1}{\sqrt{2}}(A(\tau)-B(\tau)).$$

□

Nun beweisen wir eine Aussage, die für die Beweise von MacWilliams und Gleason wichtig wird.

(3.3) Lemma
Wir definieren $f := A^4B^4(A^2-B^2)^4(A^2+B^2)^4 = A^4B^4(A^4-B^4)^4 \in \mathbb{C}[A,B]_{hom,24}$.
Dann gilt: $f = 16\Delta$, wobei $\Delta := \frac{1}{1728}(E_4^3-E_6^2)$. ◇

Beweis
Wir definieren $p := X^4Y^4(X^4 - Y^4)^4 \in \mathbb{C}[X,Y]_{hom,24}$. Nun betrachten wir die Ebene, die von A und B aufgespannt wird, indem wir A mit $(1,0)^{\mathrm{tr}}$ und B mit $(0,1)^{\mathrm{tr}}$ im $\mathbb{R}^2$ identifizieren und das Erzeugnis dieser beiden betrachten. Nun definieren wir $X := \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. Geometrisch gesehen definiert X in dieser Ebene die Transformation, welche durch eine Drehung um 45° gegen den Uhrzeigersinn, gefolgt von einer Spiegelung gegeben ist. Dann gelten die Identitäten $XA = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}(1,0)^{\mathrm{tr}} = \frac{1}{\sqrt{2}}(1,1)^{\mathrm{tr}} = \frac{1}{\sqrt{2}}(A+B)$ und $XB = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}(0,1)^{\mathrm{tr}} = \frac{1}{\sqrt{2}}(1,-1)^{\mathrm{tr}} = \frac{1}{\sqrt{2}}(A-B)$.

Durch Nachrechnen erhält man, dass f invariant unter X ist, d.h.

$$f = p(A,B) = p(XA,XB). \ (*)$$

Damit gilt nach (3.2)(iii) für $\tau \in \mathbb{H}$:

$$A\left(-\frac{1}{\tau}\right) = \left(\frac{\tau}{i}\right)^{1/2} XA(\tau) \text{ und } B\left(-\frac{1}{\tau}\right) = \left(\frac{\tau}{i}\right)^{1/2} XB(\tau) \circledast .$$

Damit folgt:

$$f\left(-\frac{1}{\tau}\right) = p(A,B)\left(-\frac{1}{\tau}\right) = A\left(-\frac{1}{\tau}\right)^4 B\left(-\frac{1}{\tau}\right)^4 \left(A\left(-\frac{1}{\tau}\right)^4 - B\left(-\frac{1}{\tau}\right)^4\right)^4$$

$$\overset{\circledast}{=} \left(\left(\frac{\tau}{i}\right)^{1/2} XA\,(\tau)\right)^4 \left(\left(\frac{\tau}{i}\right)^{1/2} XB(\tau)\right)^4 \left(\left(\left(\frac{\tau}{i}\right)^{1/2} XA\,(\tau)\right)^4 - \left(\left(\frac{\tau}{i}\right)^{1/2} XB\,(\tau)\right)^4\right)^4 .$$

$$= \left(\frac{\tau}{i}\right)^{12} (XA(\tau))^4 (XB(\tau))^4 ((XA(\tau))^4 - (XB(\tau))^4)^4$$

$$\overset{(*)}{=} \tau^{12} A(\tau)^4 B(\tau)^4 (A(\tau)^4 - B(\tau)^4)^4 = \tau^{12} p(A,B)(\tau) = \tau^{12} f(\tau).$$

Da weiterhin gilt: $q' = e^{2\pi i(\tau+1)} = e^{2\pi i\tau} e^{2\pi i} \overset{e^{2\pi i}=1}{=} e^{2\pi i\tau} = q$, folgt damit auch, dass $A(\tau+1) = A(\tau)$ und $B(\tau+1) = B(\tau)$ sind. Somit gilt:

$$f(\tau+1) = p(A,B)(\tau+1) = p(A,B)(\tau) = f(\tau).$$

Da $A = \vartheta_{\sqrt{2}\mathbb{Z}}$, ist A holomorph auf $\mathbb{H}$ und hat eine Fourier-Reihenentwicklung, die bei $n = 0$ beginnt. Da $B = \vartheta_{\frac{1}{\sqrt{2}}\mathbb{Z}} - A = \vartheta_{\frac{1}{\sqrt{2}}\mathbb{Z}} - \vartheta_{\sqrt{2}\mathbb{Z}}$ (siehe Beweis von (3.2)(iii)(a)),

gelten diese Eigenschaften auch für B und somit auch für f, da f ein Polynom in A und B ist. Damit ist insgesamt gezeigt, dass f eine Modulform vom Gewicht 12 ist.

Nun zeigen wir, dass $f = 16\Delta$ gilt.

Es gilt:

$$B(\tau) = \sum_{x \in 2\mathbb{Z}+1} q^{\frac{1}{4}x^2} = \sum_{y \in \mathbb{Z}} q^{\frac{1}{4}(4y^2+4y+1)} = q^{\frac{1}{4}} \sum_{y \in \mathbb{Z}} q^{y^2+y} = 2q^{\frac{1}{4}} + \text{ Terme höhrer Ordnung}$$

und daher auch

$$B^4(\tau) = 16q + \text{ Terme höherer Ordnung.}$$

Wegen $A = 1 + 2q + 2q^4 + 2q^9 + ...$ folgt dann auch:

$$f(\tau) = p(A, B)(\tau) = 16q + \text{ Terme höherer Ordung.}$$

D.h. f ist eine Spitzenform vom Grad 12. Da der Koeffizient von q durch 16 gegeben ist, folgt mit (1.7)(ii):

$$f = 16\Delta = 16q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

□

Es folgt als nächstes ein Satz, der uns für einen Binärcode eine weitere Darstellung für die Theta-Funktion des zugehörigen Gitters liefert.

(3.4) Satz
Sei C ein Binärcode der Länge n. Dann gilt:

$$\vartheta_{\Gamma_C} = W_C(A, B).$$

◇

Beweis
Sei $c \in C$ ein beliebiges Codewort. Dann gilt für $\tau \in \mathbb{H}$:

$$A(\tau)^{n-w(c)} B(\tau)^{w(c)} = \left(\sum_{x \in 2\mathbb{Z}} q^{\frac{1}{4}x^2} \right)^{n-w(c)} \left(\sum_{x \in 2\mathbb{Z}+1} q^{\frac{1}{4}x^2} \right)^{w(c)}$$

$$= \left(\sum_{x_i \in 2\mathbb{Z}} q^{\frac{1}{4}\left(\sum_{i=1}^{n-w(c)} x_i^2\right)} \right) \left(\sum_{x_i \in 2\mathbb{Z}+1} q^{\frac{1}{4}\left(\sum_{i=1}^{w(c)} x_i^2\right)} \right)$$

$$= \sum_{x_i \in 2\mathbb{Z},\ x_j \in 2\mathbb{Z}+1} q^{\frac{1}{4}\left(\sum_{i=1}^{n-w(c)} x_i^2 + \sum_{j=1}^{w(c)} x_j^2\right)}$$

$$= \sum_{\substack{x \in \mathbb{Z}^n, \\ |\{x_i | x_i \in 2\mathbb{Z}+1\}| = w(c)}} q^{\frac{1}{4}\left(\sum_{i=1}^{n} x_i^2\right)} = \sum_{x \in \rho^{-1}(c)} q^{\frac{1}{4}\Phi(x,x)}.$$

Damit folgt insgesamt:

$$W_C(A,B)(\tau) = \sum_{c\in C} A(\tau)^{n-w(c)}B(\tau)^{w(c)} = \sum_{c\in C}\sum_{x\in\rho^{-1}(c)} q^{\frac{1}{4}\Phi(x,x)}$$

$$= \sum_{x\in\frac{1}{\sqrt{2}}\rho^{-1}(C)} q^{\frac{1}{2}\Phi(x,x)} = \vartheta_{\Gamma_C}(\tau).$$

□

Dazu betrachten wir zunächst ein kleines

(3.5) Beispiel

(i) Wir betrachten $C :=< (1,0,0,0,0),(0,0,1,0,0),(0,0,0,0,1) >\leq \mathbb{F}_2^5$. Durch Nachrechnen erhält man, dass $W_C(X,Y) = X^5 + 3X^4Y + 3X^3Y^2 + X^2Y^3$ ist. Damit haben wir:

$$\vartheta_{\Gamma_C} = A^5 + 3A^4B + 3A^3B^2 + A^2B^3$$

(ii) Wir betrachten den erweiterten Hamming-Code $\tilde{H}$. Wir haben in (2.3)(ii) bereits gesehen, dass $W_{\tilde{H}}(X,Y) = X^8 + 14X^4Y^4 + Y^8$ gilt.

Damit folgt:

$$E_4 = \vartheta_{E_8} = \vartheta_{\Gamma_{\tilde{H}}} = A^8 + 14A^4B^4 + B^8.$$ ◇

Nun kommen wir zum ersten der beiden großen Sätze dieses Abschnitts.

(3.6) Satz (MacWilliams - Identität)
Sei C ein $[n,k,d]$-Binärcode. Dann gilt:

$$W_{C^\perp}(X,Y) = \frac{1}{2^k}W_C(X+Y, X-Y).$$

Beweis
Wir machen uns den gerade bewiesenen Satz zu Nutze und betrachten die Theta-Funktionen der Gitter. Für $\tau \in \mathbb{H}$ gilt:

$$W_C\left(A\left(-\frac{1}{\tau}\right), B\left(-\frac{1}{\tau}\right)\right) \overset{(3.4)}{=} \vartheta_{\Gamma_C}\left(-\frac{1}{\tau}\right) \overset{(1.8)}{=} \left(\frac{\tau}{i}\right)^{\frac{n}{2}} \cdot \frac{1}{\mathrm{vol}(\mathbb{R}^n/\Gamma_C)}\vartheta_{\Gamma_C^\#}(\tau)$$

$$\overset{(1.3)(ii),(v)}{=} \left(\frac{\tau}{i}\right)^{\frac{n}{2}} \cdot \frac{1}{2^{\frac{n}{2}-k}}\vartheta_{\Gamma_{C^\perp}}(\tau) \overset{(3.4)}{=} \left(\frac{\tau}{i}\right)^{\frac{n}{2}} \cdot \frac{1}{2^{\frac{n}{2}-k}}W_{C^\perp}(A(\tau),B(\tau)).$$ ⊛

Weiterhin erhalten wir mit (3.2)(iii):

$$W_C\left(A\left(-\frac{1}{\tau}\right), B\left(-\frac{1}{\tau}\right)\right) = W_C\left(\left(\frac{\tau}{i}\right)^{1/2}\frac{1}{\sqrt{2}}(A(\tau)+B(\tau)), \left(\frac{\tau}{i}\right)^{1/2}\frac{1}{\sqrt{2}}(A(\tau)-B(\tau))\right)$$
$$= \left(\frac{\tau}{i}\right)^{\frac{n}{2}} \cdot \frac{1}{2^{\frac{n}{2}}} W_C(A(\tau)+B(\tau), A(\tau)-B(\tau)). \qquad (*)$$

Indem man $\circledast$ und $(*)$ gleichsetzt und umformt, erhält man schließlich:

$$W_{C^\perp}(A,B) = \frac{1}{2^k} W_C(A+B, A-B).$$

Zudem gilt nach (3.3) und (3.5):

$$E_4 = A^8 + 14A^4B^4 + B^8 \text{ und } \Delta = \frac{1}{16}A^4B^4(A^4-B^4)^4. \quad \circledast\circledast$$

Wir wollen nun zeigen, dass A und B algebraisch unabhängig sind. Nach dem vorherigen Vortrag sind E_4 und E_6 algebraisch unabhängig und daher auch E_4 und Δ. Angenommen, A und B wären algebraisch abhängig. Dann hätte $\mathbb{C}(A,B)$ Transzendenzgrad höchstens 1. Dann würde für zwei beliebige Polynome in A und B gelten, dass diese algebraisch abhängig sind. Damit würde wegen $\circledast\circledast$ die algebraische Abhängigkeit von E_4 und Δ folgen, was ein Widerspruch wäre. Da nun A und B algebraisch unabhängig sind, folgt somit die Aussage. □

Direkt hieraus leiten wir folgenden Spezialfall ab:

(3.7) Folgerung
Sei C ein selbstdualer Binärcode der Länge n. Dann gilt:

$$W_C(X,Y) = W_C\left(\frac{X+Y}{\sqrt{2}}, \frac{X-Y}{\sqrt{2}}\right),$$

d.h. W_C ist invariant unter der Drehung um 45° gegen den Uhrzeigersinn, gefolgt von einer Spiegelung. ◇

Beweis
Es gilt:

$$W_C(X,Y) = W_{C^\perp}(X,Y) \overset{(3.6)}{=} \frac{1}{2^{\frac{n}{2}}} W_C(X+Y, X-Y) = W_C\left(\frac{X+Y}{\sqrt{2}}, \frac{X-Y}{\sqrt{2}}\right). \quad \square$$

Dazu betrachten wir ein einfaches

(3.8) Beispiel
Für $n = 4$ betrachten wir $C := \{(0,0,0,0),(1,1,0,0),(0,0,1,1),(1,1,1,1)\} \subset \mathbb{F}_2^4$. Dann ist C selbstdual und es gilt $W_C(X,Y) = X^4 + 2X^2Y^2 + Y^4$. Weiter gilt:

$$\begin{aligned} W_C\left(\frac{X+Y}{\sqrt{2}}, \frac{X-Y}{\sqrt{2}}\right) &= \left(\frac{X+Y}{\sqrt{2}}\right)^4 + 2\left(\frac{X+Y}{\sqrt{2}}\right)^2\left(\frac{X-Y}{\sqrt{2}}\right)^2 + \left(\frac{X-Y}{\sqrt{2}}\right)^4 \\ &= \frac{1}{4}X^4 + \frac{3}{2}X^2Y^2 + \frac{1}{4}Y^4 + \frac{1}{2}X^4 - X^2Y^2 + \frac{1}{2}Y^4 + \frac{1}{4}X^4 + \frac{3}{2}X^2Y^2 + \frac{1}{4}Y^4 \\ &= X^4 + 2X^2Y^2 + Y^4 = W_C(X,Y). \end{aligned}$$

◇

Als nächstes folgt der zweite große Satz dieses Abschnitts.

(3.9) Satz (Gleason)
Sei C ein doppelt gerader, selbstdualer Binärcode der Länge n. Dann ist $W_C(X,Y)$ ein Polynom in

$$\varphi := W_{\tilde{H}}(X,Y) = X^8 + 14X^4Y^4 + Y^8 \text{ und } p := X^4Y^4(X^4 - Y^4)^4,$$

in Zeichen:

$$W_C(X,Y) \in \mathbb{C}[\varphi, p].$$

Beweis
Wir beweisen die Aussage wie bei MacWilliams für A und B. Nach (3.4) wissen wir, dass $W_C(A,B) = \vartheta_{\Gamma_C}$ ist. Daher ist $W_C(A,B)$ nach (1.8) eine Modulform mit dem Gewicht $\frac{n}{2}$. Weiterhin folgt aus (1.8), dass $\frac{n}{2} \equiv 0 \pmod 4$ ist. Nun wissen wir aus (1.7)(i), dass $M \cong \mathbb{C}[E_4, E_6]$ gilt. Daraus folgt nun, dass die Modulformen vom Gewicht teilbar durch vier gegeben sind durch Polynome in E_4 und E_6^2, da hier nur Vielfache E_6 wegfallen, welche aber Gewicht 6 haben und daher nicht betrachtet werden. Daraus folgt insbesondere, dass die Menge dieser Modulformen auch isomorph zu $\mathbb{C}[E_4, \Delta]$ ist. Nach (3.3) und (3.5) gilt aber $E_4 = \varphi(A,B)$ und $\Delta = \frac{1}{16}p(A,B)$. Somit ist $W_C(A,B)$ ein Polynom in $\varphi(A,B)$ und $p(A,B)$. Da A und B algebraisch unabhängig sind, folgt die Aussage. □

Als Andeutung zum Vortrag von Herrn Pawelzik betrachten wir ein kurzes

(3.10) Beispiel
Wir betrachten den erweiterten Golay-Code $\tilde{G}$. Dann ist W_G homogen und vom Grad 24. Da φ Grad 8, p Grad 24 hat, folgt aus dem Satz von Gleason für den Gewichtszähler, dass $W_{\tilde{G}}(X,Y) = a\varphi^3 + bp$ ist für $a, b \in \mathbb{Z}$. Da für den Golay-Code

$A_4 = 0$ gilt, folgt mittels Koeffizientenvergleich, dass $42a + b = 0$ gilt. Da das Monom X^{24} nur in φ^3 auftaucht und in $W_{\tilde{G}}$ mit Koeffizient 1 auftauchen muss, folgt $a = 1$ und daher $b = -42$ und somit insgesamt:

$$W_{\tilde{G}}(X, Y) = \varphi^3 - 42p. \qquad \diamond$$

Die Polynomialdarstellung ist nicht auf E_4 und Δ beschränkt. Es sind auch andere Wahlen möglich. Ein Beispiel dafür halten wir in folgender Bemerkung fest.

(3.11) Bemerkung
Statt p kann man in (3.9) auch den Gewichtszähler des erweiterten Golay-Codes $\tilde{G}$ nehmen, denn es gilt: $p = \frac{1}{42}\varphi^3 - \frac{1}{42}W_{\tilde{G}}(X, Y)$. $\diamond$

Wir betrachten noch ein weiteres Beispiel.

(3.12) Beispiel
Sei $C \subset \mathbb{F}_2^{40}$ ein doppelt gerader, selbstdualer Code. Dann ist $W_C(X, Y)$ ein homogenes Polynom vom Grad 40. Da weiterhin X^{40} mit Koeffizient 1 als Monom auftreten muss, hat $W_C(X, Y)$ wegen Gleason die Form:

$$W_C(X, Y) = \varphi^5 + b \cdot p \cdot \varphi^2.$$

Wir nehmen weiter an, dass der minimale Abstand des Codes 8 ist, d.h. $A_4 = 0$. Da dies der Koeffizient von $X^{36}Y^4$ ist, folgt wegen obiger Gleichheit mittels Koeffizientenvergleich, dass $b = -70$ gelten muss. Weiter erhält man aus der Gleichung, dass $A_8 = 285$ ist, d.h. wir haben 285 Wörter mit minimalem Gewicht. $\diamond$

Dieses Beispiel nehmen wir zum Anlass, um Codes mit speziellem, minimalem Gewicht zu untersuchen. Dazu benutzen wir die hier bewiesenen Resultate.

§ 4 Extremale Codes und Gewichtszähler

Nun beschäftigen wir uns mit extremalen Codes und deren Gewichtszählern. Extremale Codes sind selbstduale, doppelt gerade Codes, bei denen der minimale Abstand, sprich das minimale Gewicht unter den Wörtern so groß wie möglich ist. Diese werden im letzten Vortrag genauer behandelt. Wir geben eine kleine Einführung dazu.

Wir halten zum Beginn eine kleine Bemerkung zur Struktur selbstdualer, doppelt gerader Binärcodes fest.

(4.1) Bemerkung
Sei C ein doppelt gerader und selbstdualer Binärcode. Da dann $n \equiv 0 \pmod 8$ nach (2.4) ist, gilt $n = 24m + 8k$ für ein $m \in \mathbb{N}_0$, $k \in \{0, 1, 2\}$. Nun ist W_C ein homogenes Polynom vom Grad $24m + 8k$. Mit analoger Argumentation zu (3.12) folgt wegen Gleason:

$$W_C = \sum_{j=0}^{m} b_j \varphi^{3(m-j)+k} p^j, \text{ wobei } b_j \in \mathbb{C}.$$

◇

Nun kommen wir zu einer ersten Aussage über den minimalen Abstand solcher Codes. Wir bezeichnen im Folgenden mit d den minimalen Abstand eines Codes.

(4.2) Lemma
Die Koeffizienten b_j aus (4.1) können so gewählt werden, dass $d \geq 4m + 4$ gilt. ◇

Beweis
Nach (4.1) ist $W_C = \sum_{j=0}^{m} b_j \varphi^{3(m-j)+k} p^j$. Wir zeigen nun, dass die b_j so wählbar sind, dass $A_0 = 1$ und $A_i = 0$ für alle $0 < i < 4m + 4$. Da C doppelt gerade ist, muss dies nur für alle Vielfachen von 4 gezeigt werden. Aus optischen Gründen setzen wir $X = 1$ und $Z = Y^4$, da dies keinen Einfluss auf die Aussage hat. Weiterhin lassen wir beliebige $k \in \mathbb{N}_0$ zu, da die Länge aus (4.1) dies zulässt und die Aussage dadurch im Folgenden trotzdem erhalten bleibt. Dann gilt:

$$\varphi = 1 + 14Z + Z^2 \text{ und } p = Z(1 - Z)^4.$$

Wir zeigen nun per Induktion über m, dass es zu jedem $m \in \mathbb{N}_0$ Koeffizienten $b_0, \ldots, b_m \in \mathbb{C}$ gibt, sodass für alle $k \in \mathbb{N}_0$ gilt: $W_C = 1 + 0 + \ldots + 0 + cZ^{m+1} + \ldots$.

(IA) Sei $m = 0$. Dann gilt für $k \in \mathbb{N}_0$:

$$W_C = \sum_{j=0}^{0} b_j \varphi^{3(0-j)+k} p^j = b_0 \varphi^k \cdot p^0 = b_0 \varphi^k = b_0 (1 + 14Z + Z^2)^k$$

$$= b_0 (1 + 14kZ + \text{ Terme höherer Ordnung}).$$

Wir setzen $b_0 = 1$ und erhalten das Gewünschte.

(IS) $(m \to m + 1)$ Für $k \in \mathbb{N}_0$ gilt:

$$W = \sum_{j=0}^{m+1} b_j \varphi^{3(m+1-j)+k} p^j = \sum_{j=0}^{m} b_j \varphi^{3(m+1-j)+k} p^j + b_{m+1} \varphi^k p^{m+1}$$

$$= \underbrace{\sum_{j=0}^{m} b_j \varphi^{3(m-j)+(k+3)} p^j}_{=:\psi} + b_{m+1} \varphi^k p^{m+1}$$

Nach Induktionsvoraussetzung existieren $b_0, \dots b_m \in \mathbb{C}$, sodass gilt:

$$\psi = 1 + 0 + \dots + 0 + cZ^{m+1} + \text{ Terme höherer Ordnung.}$$

Des Weiteren erhält man durch Ausmultiplizieren:

$$\varphi^k p^{m+1} = Z^{m+1} + \text{ Terme höherer Ordnung.}$$

Nun setzen wir $b_{m+1} = -c$ und erhalten das erwünschte Resultat.

Insgesamt haben wir also gezeigt, dass eine Wahl von Koeffizienten gibt, sodass $A_0 = 1$ und $A_i = 0$ für $0 < i < 4m + 4$ gilt. Damit folgt die Behauptung. □

Nun halten wir eine weitere Aussage über d fest.

(4.3) Satz
Für C wie in (4.1) gilt $A_{4m+4} \neq 0$. Genauer gilt:

(i)

$$A_{4m+4} = \binom{n}{5}\binom{5m-2}{m-1} \Big/ \binom{4m+4}{5}, \text{ falls } n = 24m,$$

(ii)

$$A_{4m+4} = \frac{1}{4}n(n-1)(n-2)(n-4)\frac{(5m)!}{m!(4m+4)!}, \text{ falls } n = 24m+8,$$

(iii)

$$A_{4m+4} = \frac{3}{2}n(n-2)\frac{(5m+2)!}{m!(4m+4)!}, \text{ falls } n = 24m+16.$$

◇

Der Beweis dazu erfordert Theorie, die wir noch nicht zur Verfügung haben (unter anderem die der Designs, welche im nächsten Vortrag kommt) und sprengt den Rahmen dieses Vortrags. Er lässt sich nachlesen in Kapitel 19, Abschnitt 5 von [2].

Nun kommen wir zu der eigentlichen Definition extremaler Codes.

(4.4) Definition
Sei $C \subset \mathbb{F}_2^n$ ein Binärcode wie in (4.1). Dann heißt C extremal, falls $d = 4m + 4$ gilt. Der zugehörige Gewichtszähler W_C heißt dann extremaler Gewichtszähler. ◇

Nun betrachten wir einige Beispiele.

(4.5) Beispiel

(i) Sei $n = 24$, d.h. $m = 1, k = 0$. Dann gilt $A_8 = 759$. Dies haben wir bereits in (2.7) gesehen. Im nächsten Vortrag wird gezeigt, dass ein extremaler Code der Länge 24 existiert und durch den erweiterten Golay-Code $\tilde{G}$ eindeutig bestimmt ist.

(ii) Für $n = 48$, d.h $k = 0, m = 2$ folgt mit der Formel, dass $A_{12} = 17296$ ist, d.h. falls ein extremaler Code der Länge 48 existiert, hat er 17296 Wörter mit minimalem Gewicht.

(iii) Für $n = 72$, d.h $k = 0, m = 3$ folgt mit der Formel, dass $A_{16} = 249849$ ist, d.h. falls ein extremaler Code der Länge 48 existiert, hat er 249849 Wörter mit minimalem Gewicht. ◇

Wir beenden den Abschnitt mit der Bemerkung, dass gezeigt werden kann, dass $A_{m+8} < 0$ für $n = 24m$ hinreichend groß (etwa bei $n = 3720$) gilt. Daraus folgt, dass extremale Codes nur für endlich viele Längen existieren können. Für $n \leq 64$ ist die Existenz bekannt sowie für einige $n > 72$. Für $n = 72$ ist die Existenz unbekannt. Vergleichbare Aussagen kann man auch über Gitter treffen, indem man extremale Gitter betrachtet. Dies wird im Vortrag über extremale Gitter und Codes weiter ausgeführt.

Literatur

[1] W. Ebeling, Lattices and Codes - A Course Partially Based on Lectures by Friedrich Hirzebruch, Springer, 3. Auflage, 2013.

[2] F. J. MacWilliams und N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1988