Konstruktion extremaler Gitter und Codes nach Turyn und Quebbemann

Christian Doberstein und Dirk Liebhold

RWTH - 27.05.2013

1 Codes

1.1 Einleitung

Im Folgenden beschreiben wir eine Möglichkeit, aus gegebenen Codes neue zu konstruieren. Wir werden diese Konstruktion daraufhin nutzen, um aus dem erweiterten Hamming-Code extremale Typ II Codes der Längen $16, 24, 32$ und 40 zu konstruieren. In den Beispielen geben wir Codes immer durch ihre Erzeugermatrizen an. Ist also C ein Code und M eine Matrix, so steht $C = M$ dafür, dass C der Zeilenraum von M ist.

1.2 Grundbegriffe

Definition 1.1
Die Abbildung $b : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2, (x, y) \mapsto \sum_{i=1}^n x_i y_i$ ist eine Bilinearform auf $\mathbb{F}_2^n$.
Identifizieren wir $\mathbb{F}_2$ mit $\{0, 1\} \subseteq \mathbb{Z}$, so definieren wir $B : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{Z}, (x, y) \mapsto \sum_{i=1}^n x_i y_i$ und $w : \mathbb{F}_2^n \to \mathbb{Z}, x \mapsto B(x, x)$.

Klar: $B(x, y) \equiv b(x, y) (\mathrm{mod}\ 2)$ für alle $x, y \in \mathbb{F}_2^n$.
Mit $w(x)$ bezeichnen wir das Gewicht eines Vektors $x \in \mathbb{F}_2^n$.

Definition 1.2
Eine Abbildung $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ heißt Isometrie, wenn φ ein Isomorphismus ist und $w(\varphi(x)) = w(x)$ für alle $x \in \mathbb{F}_2^n$ gilt.
Ist $C \leq \mathbb{F}_2^n$ ein Code, so heißt $\varphi(C)$ ein zu C isometrischer Code.

Lemma 1.3
Es ist φ genau dann eine Isometrie, wenn φ eine Permutation der Koordinaten beschreibt.

Beweis: Sei $(e_1, \ldots, e_n)$ die Standardbasis von $\mathbb{F}_2^n$. Dann gilt $w(x) = 1$ genau dann wenn $x = e_i$ für ein i, es muss also für alle $1 \leq i \leq n$ gelten: $\varphi(e_i) \in \{e_1, \ldots, e_n\}$. Da φ bijektiv ist, induziert φ also eine Permutation der e_i, also eine Permutation der Koordinaten. Auf der anderen Seite ist jede Permutation der Koordinaten ein Isomorphismus, der das Gewicht eines jeden Vektors erhält; also eine Isometrie. □

Definition 1.4
Sei $C \leq \mathbb{F}_2^n$ ein Code.
Ist $w(x) \in 2\mathbb{Z}$ für alle $x \in C$, so heißt C gerade.
Ist $w(x) \in 4\mathbb{Z}$ für alle $x \in C$, so heißt C doppelt gerade.
Ist $C \subseteq C^\perp$, so heißt C selbstorthogonal. Gilt Gleichheit so nennt man C selbstdual.
Mit $w(C) := \min\{w(x) \mid 0 \neq x \in C\}$ bezeichnen wir das Minimalgewicht des Codes C.

Das Minimalgewicht lässt sich wie folgt berechnen.

Lemma 1.5
Sei $0 \neq C \leq \mathbb{F}_2^n$ ein Code der Dimension k und H eine Kontrollmatrix von C - das heißt $H \in \mathbb{F}_2^{(n-k)\times n}$ eine Matrix mit vollem Rang und $C = \text{Kern}(H)$.
Dann ist $w(C)$ die minimale Anzahl linear abhängiger Spalten in H.

Beweis: Da $k > 0$ besitzt H linear abhängige Spalten. Sei also m die minimale Anzahl abhängiger Spalten in H. Nach Lemma (1.3) sind alle Permutationen der Koordinaten Isometrien, ändern also insbesondere nicht das Minimalgewicht. Damit können wir oBdA annehmen, dass die ersten m Spalten von H linear abhängig sind, jedoch keine $m-1$ der ersten m Spalten. Das bedeutet, dass der Vektor $\begin{pmatrix} 1^m & 0^{n-m} \end{pmatrix}$ im Kern von H, also in C liegt. Damit folgt $w(C) \leq m$. Umgekehrt sei $v \in C$ mit $v \neq 0$ und $a := w(v)$ minimal. Dann stellt $v \in \text{Kern}(H)$ eine lineare Abhängigkeit von a Spalten von H dar und es folgt $a \geq m$. □

Wir werden ab nun überwiegend doppelt gerade selbstduale Codes (kurz: Typ II Codes[1]) betrachten. Ist C ein Typ II Code, so ist $C = C^\perp$. Da $(\mathbb{F}_2^n, b)$ regulär ist folgt damit sofort $\dim(C) = \frac{n}{2}$, insbesondere ist n gerade.

1.3 Konstruktion

Bei der folgenden Konstruktion, die auf Turyn zurück geht, identifizieren wir das Tensorprodukt zweier Vektoren mit ihrem Kroneckerprodukt. Dadurch können wir $\mathbb{F}_2^n \otimes \mathbb{F}_2^m \cong \mathbb{F}_2^{nm}$ schreiben.

[1] vergleiche [9]

Satz 1.6
Seien $C_1, \dots, C_k \leq \mathbb{F}_2^n$ und $X_1, \dots, X_k \leq \mathbb{F}_2^m$ Codes und es gelte $\mathbb{F}_2^m = X_1 \oplus X_2 \oplus \dots \oplus X_k$.
Dann ist $T := T(C_i, X_i) := \bigoplus_{i=1}^{k} X_i \otimes C_i \leq \mathbb{F}_2^{mn}$ ebenfalls ein Code.
Sind alle C_i selbstorthogonal,selbstdual oder Typ II, so hat T die jeweilige Eigenschaft ebenfalls.

Für den Beweis benötigen wir zuerst ein kleines Hilfslemma.

Lemma 1.7
Seien $c, d \in \mathbb{F}_2^n$ und $x, y \in \mathbb{F}_2^m$. Dann ist $b(x \otimes c, y \otimes d) = b(x, y) \cdot b(c, d)$ und $w(x \otimes c) = w(x)w(c)$.

Beweis: Mit dem Kroneckerprodukt ist $x \otimes c = \begin{pmatrix} x_1 c & x_2 c & \dots & x_m c \end{pmatrix}$ sowie $y \otimes d = \begin{pmatrix} y_1 d & \dots & y_m d \end{pmatrix}$. Damit ist $b(x \otimes c, y \otimes d) = \sum_{i=1}^{m} \sum_{k=1}^{n} x_i y_i c_k d_k = \sum_{i=1}^{m} x_i y_i \sum_{k=1}^{n} c_k d_k = \sum_{i=1}^{m} x_i y_i b(c, d) = b(x, y) \cdot b(c, d)$.
Dass $w(x \otimes c) = w(x)w(c)$ ist, folgt ebenfalls aus der Form von $x \otimes c$. □

Beweis von Satz (1.6): Seien alle C_i selbstorthogonal. Es reicht zu zeigen, dass die Erzeuger von T senkrecht aufeinander stehen. Haben wir $c \in C_i$, $d \in C_j$ sowie $x \in X_i$, $y \in X_j$ so ist $b(x \otimes c, y \otimes d) = b(x, y)b(c, d) = 0$, denn für $i = j$ ist $b(c, d) = 0$ und für $i \neq j$ ist $b(x, y) = 0$.
Nun angenommen, dass alle C_i selbstdual sind. Dann gilt $\dim(C_i) = \frac{n}{2}$ und da das Tensorprodukt direkte Summen erhält, erhalten wir $\dim(T) = \sum_{i=1}^{m} \dim(X_i)\frac{n}{2} = \frac{mn}{2}$. Da wir $T \subseteq T^\perp$ bereits gesehen haben, folgt jetzt aus Dimensionsgründen die Gleichheit, also ist T selbstdual.
Sind zu guter Letzt alle C_i Typ II, das heißt selbstdual und doppelt gerade, so haben auch alle Erzeuger von T ein Gewicht in $4\mathbb{Z}$ und damit ist dann auch T ein Typ II Code.
□

Beispiel: Seien C und D gegeben durch

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}, D = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

und X durch $X = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$. Es sind C, D Typ II (genauer isomorph zum erweiterten Hamming-Code) und $T(C, D, X, X^\perp) \leq \mathbb{F}_2^{24}$ ist isomorph zum Golay-Code. Dies entspricht Turyns ursprünglicher Konstruktion[2], die wir in dieser Arbeit verallgemeinern.

[2] vergleiche [6] Seite 588

Sowohl der erweiterte Hamming-Code als auch der Golay-Code sind besondere Typ II Codes, sogenannte extremale Codes. Diese haben eine besonders hohe Minimaldistanz, die nützlich für das Dekodieren eventuell mit Fehlern behafteter Nachrichten ist.

Definition 1.8 *([7, 8])*
Ist C ein Typ II Code, so gilt immer $d(C) \leq 4 + 4\left\lfloor \frac{n}{24} \right\rfloor$. Gilt Gleichheit, so nennt man C extremal.

Es sind bisher extremale Typ II Codes in $\mathbb{F}_2^n$ für $n = 8, 16, 24, 32, 40, 48, 56, 64$ bekannt. Weiterhin existieren extremale Typ II Codes nicht, sobald $n \geq 3952$[3].

Wir untersuchen nun, wie wir systematisch extremale Typ II Codes konstruieren können. Dazu benötigen wir den Einsvektor $\mathbb{1} := \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix} \in \mathbb{F}_2^n$.

Lemma 1.9
Sind C_i Typ II Codes, so gilt $w(T) \leq n$. Eine genauere obere Schranke ist $\min_{\emptyset \neq I \subseteq \{1,\dots,k\}} w(\bigcap_{i\in I} C_i) \cdot w(\bigoplus_{i\in I} X_i)$.

Beweis: Sei $v = \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix} \in \mathbb{F}_2^m$. Da $\mathbb{F}_2^m = \bigoplus_{i=1}^{k} X_i$, liegt v damit in der Summe der X_i. Da die C_i Typ II Codes sind, enthalten sie alle den Vektor $\mathbb{1}$ und damit gilt $v \otimes \mathbb{1} \in T$. Mit Lemma (1.7) ergibt sich $w(v \otimes \mathbb{1}) = 1 \cdot n = n$, also ist $w(T) \leq n$.
Für die zweite obere Schranke sei $\emptyset \neq I \subseteq \{1, \dots, k\}$ beliebig. Seien $v \in \bigoplus_{i\in I} X_i$ und $c \in \bigcap_{i\in I} C_i$ jeweils Vektoren ungleich 0 mit minimalem Gewicht. Wie im ersten Teil ist dann $v \otimes c \in T$ und es gilt wieder $w(v \otimes c) = w(v)w(c)$. Da wir für alle $I \subseteq \{1, \dots, k\}$ eine obere Schranke an $w(T)$ erhalten, ist $w(T)$ auch durch das Minimum nach oben beschränkt. □
Diese Tatsache sagt uns bereits, dass das Finden extremaler Codes mit der in Satz (1.6) beschriebenen Konstruktion nur dann möglich ist, wenn $m \leq 5$ gilt. Außerdem sollte $w(C_i \cap C_j)$ für alle $i \neq j$ möglichst groß sein. Dies ist für Typ II Codes gegeben, wenn $\dim(C_i \cap C_j) = 1$, denn dann enthält $C_i \cap C_j$ nur den Nullvektor und den Einsvektor, also $w(C_i \cap C_j) = n$.
Sollten wir es mit Codes zu tun haben, bei denen $\dim(C_i \cap C_j) > 1$ für manche i, j, so sollte $w(X_i + X_j)$ in diesem Fall möglichst groß gewählt werden. Dass diese Überlegung relevant und bei mehr als 2 Codes unumgänglich ist, zeigt das folgende Lemma.

Lemma 1.10
Seien C, D, E Typ II Codes mit $\dim(C \cap D) = \dim(C \cap E) = 1$. Dann gilt $\dim(D \cap E) \geq 2$.

[3] vergleiche [11]

Beweis: Da C, D, E Typ II Codes sind, gilt $\mathbb{1} \in C, D, E$ und $C, D, E \subseteq \langle \mathbb{1} \rangle^\perp$. Wir können also C, D, E als Unterräume von $V := \langle \mathbb{1} \rangle^\perp / \langle \mathbb{1} \rangle$ auffassen und werden dies ab jetzt auch tun. Auf V ist durch $q : V \to \mathbb{F}_2, x + \langle \mathbb{1} \rangle \mapsto \frac{w(x)}{2} + 2\mathbb{Z}$ eine quadratische Form definiert und C, D, E sind maximal isotrope Teilräume von V. Das und die Tatsache, dass $V = C \oplus D$ gilt, erlaubt es, Basen $(c_1, \ldots, c_k)$ von C und $(d_1, \ldots, d_k)$ von D zu finden, sodass $q(c_i) = q(d_i) = 0$ für alle i, $b_q(c_i, c_j) = b_q(d_i, d_j) = 0$ für alle i, j und schließlich $b_q(c_i, d_j) = \delta_{ij}$, ebenfalls für alle i, j. Hierbei ist b_q die von q induzierte Bilinearform, sodass $q(x+y) = q(x) + q(y) + b_q(x, y)$ für alle $x, y \in V$ gilt. Eine Basis von E hat nun die Form $(e_1, \ldots, e_k)$ mit $e_i = d_i + a_i$ mit $a_i \in C$, also $a_i = \sum_{j=1}^{k} a_{ij} c_j$ für geeignete $a_{ij} \in \mathbb{F}_2$. Angenommen in V gelte $D \cap E = \{0\}$. Dann müssen die a_i eine Basis von C bilden und die Matrix A definiert durch $A_{ij} = a_{ij}$ wäre als Basiswechselmatrix invertierbar.
Nun verwenden wir, dass auch E ein isotroper Teilraum von V ist, dass also $q(e_i) = b_q(e_i, e_j) = 0$ für alle i, j. Wir erhalten $0 = q(e_i) = q(d_i + a_i) = q(d_i) + q(a_i) + b_q(d_i, a_i) = a_{ii}$ sowie $0 = b_q(e_i, e_j) = b_q(d_i + a_i, d_j + a_j) = b_q(d_i, d_j) + b_q(d_i, a_j) + b_q(a_i, d_j) + b_q(a_i, a_j) = b_q(d_i, a_j) + b_q(a_j, d_i) = a_{ji} + a_{ij}$. Damit ist A schiefsymmetrisch. Nun ist aber A eine $k \times k$ Matrix und $k = \frac{n-2}{2}$. Mit dem folgenden Lemma ist k ungerade und damit kann A nicht vollen Rang haben, also keine Basiswechselmatrix sein, und es folgt $D \cap E \neq \{0\}$ in V. □

Lemma 1.11
Sei $C \leq \mathbb{F}_2^n$ ein Typ II Code. Dann ist $n \in 4\mathbb{Z}$.

Beweis: Da C doppelt gerade ist, ist $C \subseteq \langle \mathbb{1} \rangle^\perp$. Da C selbstdual ist, folgt $\mathbb{1} \in C$ und damit - wieder da C doppelt gerade - $n = w(\mathbb{1}) \in 4\mathbb{Z}$. □

Aus der Theorie quadratischer Formen ist bekannt, dass extremale Codes genau dann in $\mathbb{F}_2^n$ existieren, wenn $n \in 8\mathbb{Z}$.

Beispiele: Seien C, D, E wie folgt definiert.

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}, \quad D = E = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Diese Codes sind isometrisch zum erweiterten Hamming-Code, also Typ II Codes. Weiterhin gilt $\dim(C \cap D) = \dim(C \cap E) = 1$ sowie $w(D \cap E) = 4$.
Wir wählen die folgenden orthogonalen Zerlegungen des $\mathbb{F}_2^k$ für $k = 2, 3, 4, 5$:

$$A_1 = \begin{pmatrix} 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$X_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, X_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$Y_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, Y_2 = \begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix}, Y_3 = \begin{pmatrix} 1 & 1 & 1 & 0 \end{pmatrix}$$

$$Z_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}, Z_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}, Z_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Kombinieren wir nun jeweils C, D beziehungweise C, D, E mit den orthogonalen Zerlegungen, so erhalten wir - wie eine kurze Rechnung in Magma ([1]) zeigt - extremale Typ II Codes der Längen $16, 24, 32$ und 40.

2 Gitter

2.1 Motivation

In diesem Abschnitt widmen wir uns einer Konstruktion von Gittern, die von H.-G. Quebbemann stammt ([10]), mit dem Ziel, Gitter mit einem möglichst großem Minimum zu konstruieren. Interpretieren wir die Gitterpunkte als Mittelpunkte von Kugeln mit gleichem, maximalen Radius ohne das sich die Kugeln überschneiden, so können auf diese Weise durch Gitter Kugelpackungen im $\mathbb{R}^n$ beschrieben werden. Allgemeiner wird eine beliebige überschneidungsfreie Anordnung von Kugeln im $\mathbb{R}^n$ als Kugelpackung bezeichnet, wobei eine solche Anordnung im Allgemeinen nicht mehr durch ein Gitter beschrieben werden kann. Das klassische Problem der dichtesten Kugelpackung ist für $n = 1$ trivial lösbar, wurde für $n = 2$ von Fejes Tóth und für $n = 3$ von T. C. Hales ([4]) gelöst, ist aber schon für $n \geq 4$ ungelöst. Die dichteste, von einem Gitter induzierte Kugelpackung, ist hingegen bis $n = 8$ bekannt. Es stellt sich nun heraus, dass das Minimum eines Gitters im Wesentlichen proportional zu der Dichte der resultierenden Kugelpackung ist, weshalb es berechtigt ist bei einem großen Minimum eines Gitters eine hohe Dichte der Kugelpackung zu erwarten.

2.2 Einleitung

Ähnlich wie wir uns in dem ersten Teil auf Codes über dem Grundkörper $\mathbb{F}_2$ beschränkt haben, wollen wir auch Gitter nicht in ihrer allgemeinsten Form betrachten und beschränken uns auf Gitter über dem Grundring $\mathbb{Z}$.

Definition 2.1
Sei $n \in \mathbb{N}$ und $V := (\mathbb{R}^n, q)$ ein reeller quadratischer Vektorraum. Ein Gitter in V ist ein freier $\mathbb{Z}$-Modul $L \subseteq V$ vom Rang n zusammen mit der auf L eingeschränkten quadratischen Form $q|_L : L \to \mathbb{R}$.

Die durch eine quadratische Form $q : \mathbb{R}^n \to \mathbb{R}$ definierte Bilinearform $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}, (x, y) \mapsto q(x + y) - q(x) - q(y)$ werden wir im Folgenden kurz mit b_q bezeichnen. Ein Gitter L nennen wir ganz, wenn $b_q(L, L) \subseteq \mathbb{Z}$ ist und gerade, wenn $b_q(x, x) \in 2\mathbb{Z}$ für alle $x \in L$ gilt. Da $b_q(x, x) = 2q(x)$ für alle $x \in L$ gilt, liegen für ein gerades Gitter L die Werte der quadratischen Form $q|_L$ offenbar in $\mathbb{Z}$ und aus der Definition von b_q folgt unmittelbar, dass gerade Gitter ganz sind. Ein Gitter L heißt positiv definit, wenn die Bilinearform b_q positiv definit ist.

Definition 2.2
Das zu einem Gitter L duale Gitter ist gegeben durch

$$L^{\#} = \{x \in L \otimes \mathbb{R} \mid b_q(x, L) \subseteq \mathbb{Z}\}.$$

Ist B eine Basis von L, so ist die zu B duale Basis eine Basis von $L^{\#}$. Für ein ganzes Gitter L gilt $L \subseteq L^{\#}$ und $L^{\#}/L$ ist eine endliche abelsche Gruppe, welche Diskriminantengruppe von L heißt. Ein Gitter mit trivialer Diskriminantengruppe, d.h. $L = L^{\#}$, ist unimodular.

Sei L nun ein ganzes Gitter in dem reellen quadratischen Vektorraum $(\mathbb{R}^n, q)$.

Definition 2.3
Das Minimum von L ist gegeben durch

$$\min(L) \coloneqq \min_{0 \neq x \in L} q(x) \ .$$

Der Zusammenhang zwischen dem Minimum eines Gitters und der Dichte der entsprechenden Kugelpackung ergibt sich nun aus

$$\mathrm{D}(L) = \left(\frac{\mu(L)}{4}\right)^{\frac{n}{2}} \cdot \mathrm{vol}(S_n) = \frac{\left(\frac{1}{2}\min(L)\right)^{\frac{n}{2}} \cdot \mathrm{vol}(S_n)}{\sqrt{\left|L^{\#}/L\right|}},$$

wobei $\mathrm{D}(L)$ die Dichte der Kugelpackung, $\mathrm{vol}(S_n)$ das Volumen der n-dimensionalen Einheitskugel und $\mu(L)$ die Minkowski-Zahl

$$\mu(L) \coloneqq \frac{2\min(L)}{\sqrt[n]{\left|L^{\#}/L\right|}}$$

bezeichnet. Offenbar hängt die Dichte der Kugelpackung in gegebener Dimension n lediglich von der Minkowski-Zahl des Gitters ab. Schränken wir uns auf die Betrachtung unimodularer Gitter ein, so ergibt sich als weitere Vereinfachung, dass $\mathrm{D}(L)$ jetzt ausschließlich von dem Minimum von L abhängt. Das Minimum eines unimodularen geraden Gitters L ist durch $\lfloor \frac{n}{24} \rfloor + 1$ nach oben beschränkt ([8]). Unimodulare gerade Gitter L mit $\min(L) = \lfloor \frac{n}{24} \rfloor + 1$ heißen extremale Gitter.

2.3 Konstruktion

Sei (L, q) ein positiv definites gerades Gitter von geradem Rang $n \in 2\mathbb{N}$. Für die folgende Konstruktion müssen wir zunächst eine Polarisation von L ermitteln, d.h. zu einer Primzahl p zwei $\mathbb{Z}$-Moduln M, N bestimmen, sodass $(M, \frac{1}{p}q)$ und $(N, \frac{1}{p}q)$ wieder gerade Gitter mit derselben Diskriminantengruppe wie L sind und zudem $L = N + M$ sowie $pL = N \cap M$ erfüllen.

Dazu wählen wir zunächst $p \in \mathbb{P}$ teilerfremd zu $\left|L^\# / L\right|$. Dann ist die durch q induzierte quadratische Form

$$\bar{q} : L/pL \to \mathbb{Z}/p\mathbb{Z},\ x + pL \mapsto q(x) + p\mathbb{Z}$$

nicht ausgeartet, da

$$b_{\bar{q}}(\bar{x}, L/pL) = 0 \iff b_q(x, L) \subseteq p\mathbb{Z} \iff b_q(\frac{x}{p}, L) \subseteq \mathbb{Z} \iff \frac{x}{p} \in L^\#,$$

was wegen $p \nmid \left|L^\# / L\right|$ aber $\frac{x}{p} \in L$, also $\bar{x} = 0$ impliziert. Damit ist $(L/pL, \bar{q})$ eine reguläre quadratische Form über $\mathbb{Z}/p\mathbb{Z}$ und aus der Klassifikation regulärer quadratischer Formen über endlichen Körpern ist bekannt ([5]), dass

$$(L/pL, \bar{q}) \cong \overset{n/2}{\underset{i=1}{\perp}} \mathbb{H} \quad \text{oder} \quad (L/pL, \bar{q}) \cong N(\mathbb{F}_p) \perp \overset{n/2-1}{\underset{i=1}{\perp}} \mathbb{H}\ .$$

In dem ersten Fall ist $(L/pL, \bar{q})$ hyperbolisch, also gibt es singuläre $A, A' \leq L/pL$ mit $A = A^\perp$, $A' = (A')^\perp$ und $L/pL = A \oplus A'$. Um daraus eine Polarisation von L zu erhalten, liften wir A und A' wieder nach $L \otimes \mathbb{R}$, d.h. wir setzen $M := \varphi^{-1}(A)$ und $N := \varphi^{-1}(A')$, wobei $\varphi : L \to L/pL$ die kanonische Surjektion ist. Dann gilt $L = M + N$ sowie $pL = M \cap N$ und dass $(M, \frac{1}{p}q)$ sowie $(N, \frac{1}{p}q)$ wieder gerade Gitter sind folgt unmittelbar daraus, dass A und A' singulär sind. Weiter ist $\left|L^\# / L\right| = \left|M^\# / M\right|$ und wegen $M \subseteq L \subseteq L^\# \subseteq M^\#$ gilt $L^\# / L \leq M^\# / M$, also stimmt die Diskriminantengruppe von M mit der Diskriminantengruppe von L überein. Analog zeigt man $L^\# / L = N^\# / N$.

Mithilfe der Polarisation von L können wir nun die allgemeine Konstruktionsvorschrift formulieren:

Satz 2.4 *([10])*
Sei B eine Untergruppe von A^m, $m \in \mathbb{N}$, und

$$B' := (A')^m \cap B^\perp = \left\{ (z_1, \ldots, z_m) : z_i \in A', \sum_{i=1}^{m} b_{\bar{q}}(b_i, z_i) = 0 \ \ \forall \ \ (b_1, \ldots, b_m) \in B \right\}.$$

Setzen wir $C := B \oplus B' \leq (L/pL)^m$, so gilt $\bar{q}^m(C) = \{0\}$, $C = C^\perp$ und

$$\Lambda := \Lambda(L, A, A', B) := \{x \in L^m \mid \bar{x} \in C\}$$

mit der quadratischen Form $\hat{q} := \frac{1}{p} q^m$ ist ein Gitter mit Diskriminantengruppe $\Lambda^\# / \Lambda \cong (L^\# / L)^m$. Ist (L, q) unimodular, so ist auch $(\Lambda, \hat{q})$ wieder unimodular.

Beweis: Direkt aus der Definition von B und B' folgt $\bar{q}^m(C) = \{0\}$, was $b^m_{\bar{q}}(C, C) = \{0\}$ und damit $C \subseteq C^\perp$ impliziert. Betrachten wir C nun als $\mathbb{F}_p$-Vektorraum, so folgt aus

$$\begin{aligned} \dim(C) &= \underbrace{\dim(B)}_{=:k} + \dim(B') = k + \dim(B^\perp) - \dim(B^\perp \cap A^m) \\ &= k + (nm - k) - \frac{nm}{2} = \frac{nm}{2} \end{aligned}$$

die Gleichheit, d.h. $C = C^\perp$. Da $\mathbb{Z}$ ein Hauptidealbereich ist, ist Λ endlich erzeugt (als Untermodul des endlich erzeugten $\mathbb{Z}$-Moduls L^m vom Rang nm kann Λ von nm Elementen erzeugt werden) und torsionsfrei, also frei. Wegen $\bar{q}^m(C) = \{0\}$ ist $q^m(\Lambda) \subseteq p\mathbb{Z}$ und somit $\hat{q}$ wohldefiniert. Die letzte Behauptung folgt aus

$$\Lambda^\# / \Lambda = (L^m)^\# / L^m \cong (L^\# / L)^m \, . \qquad \square$$

Bevor wir auf diese Art und Weise jetzt Gitter konstruieren, betrachten wir noch zwei Spezialfälle der obigen Konstruktionsvorschrift, welche sich aufgrund ihrer Struktur leicht untersuchen lassen.

Lemma 2.5 *(Konstruktion I, [10])*
Wählen wir $B = \{(x, \ldots, x) \mid x \in A\} \leq A^m$, so gilt

$$B' = \left\{ (z_1, \ldots, z_m) : z_i \in A' \text{ und } \sum\nolimits_{i=1}^{m} z_i = 0 \right\}.$$

Das so gebildete Gitter $\Lambda(L, A, A', B)$ bezeichnen wir mit $\Lambda(L, A, A', m)$ oder $\Lambda(L, M, N, m)$.

Beweis: Sei $(z_1, \ldots, z_m) \in (A')^m$. Da $b_{\bar{q}}$ nicht ausgeartet ist, gilt $0 = \sum_{i=1}^m b_{\bar{q}}(x, z_i) = b_{\bar{q}}(x, \sum_{i=1}^m z_i)$ für alle $x \in A$ genau dann, wenn $\sum_{i=1}^m z_i = 0$ ist. $\square$

Lemma 2.6 *(Konstruktion II, [10])*
Seien $\sigma_1, \ldots, \sigma_m$ Endomorphismen von A und $B = \{(x+\sigma_1(y), \ldots, x+\sigma_m(y)) \mid x, y \in A\}$. Dann ist

$$B' = \left\{(z_1, \ldots, z_m) : z_i \in A' \text{ mit } \sum_{i=1}^m z_i = \sum_{i=1}^m \sigma_i^*(z_i) = 0\right\},$$

wobei σ_i^* den zu σ_i adjungierten Endomorphismus auf A' bezüglich $b_{\bar{q}}$ bezeichnet.

Offenbar geht die Konstruktion I als Spezialfall $\sigma_1 = \ldots = \sigma_m = \mathrm{id}_A$ aus der Konstruktion II hervor.

Beweis: Sei $(z_1, \ldots, z_m) \in (A')^m$. Analog zu Lemma (2.5) gilt $0 = \sum_{i=1}^m b_{\bar{q}}(x+\sigma_i(y), z_i) = b_{\bar{q}}(x, \sum_{i=1}^m z_i) + b_{\bar{q}}(y, \sum_{i=1}^m \sigma_i^*(z_i))$ für alle $x, y \in A$ genau dann, wenn $\sum_{i=1}^m z_i = \sum_{i=1}^m \sigma_i^*(z_i) = 0$ ist. □

Das folgende Lemma liefert eine Abschätzung für die Minima der gemäß Konstruktion I gebildeten Gitter $\Lambda(L, M, N, k)$, welche sich nachher in den Beispielen als nützlich erweisen wird.

Lemma 2.7
Sei (M, N) eine Polarisation von (L, q) bezüglich $p \in \mathbb{P}$ und $k \in \mathbb{N}$. Wenn $d := \min(L, q) = \min(M, \frac{1}{p}q) = \min(N, \frac{1}{p}q)$ ist, gilt

$$\min\left\{2d, \left\lceil \frac{kd}{p} \right\rceil\right\} \leq \min(\Lambda(L, M, N, k), \hat{q}) \leq pd$$

Beweis: Aus Satz (2.4) und Lemma (2.5) ergibt sich, dass wir das Gitter Λ explizit durch

$$\Lambda = \left\{(m + n_1, \ldots, m + n_k) : m \in M, n_i \in N, \sum_{i=1}^k n_i \in pL\right\}$$

angeben können. Sei $0 \neq \lambda \in \Lambda$ beliebig. Wir unterscheiden drei Fälle, wobei die von Null verschiedenen Einträge von $\lambda \in \Lambda \subseteq L^k$ oBdA die führenden Einträge seien:
1.Fall: $\lambda = (\lambda_1, 0, \ldots, 0)$, $\lambda_1 \neq 0$. Dann ist $\lambda_1 = px \in pL$ für ein $x \in L$ und somit $\hat{q}(\lambda) = \frac{1}{p}q(px) = pq(x) \geq pd \geq 2d$.
2.Fall: $\lambda = (\lambda_1, \ldots, \lambda_s, 0, \ldots, 0)$, $\lambda_i \neq 0 \ \forall\ i \in \{1, \ldots, s\}$ und $s \geq 2$. Hier haben wir $\lambda_1, \ldots, \lambda_s \in N$, also ist $\hat{q}(\lambda) = \sum_{i=1}^s \frac{1}{p}q(\lambda_i) \geq sd \geq 2d$.
3.Fall: $\lambda = (\lambda_1, \ldots, \lambda_k)$, $\lambda_i \neq 0 \ \forall\ i$. In diesem Fall gilt $\hat{q}(\lambda) = \frac{1}{p}\sum_{i=1}^k q(\lambda_i) \geq \frac{1}{p}kd$.
Für die obere Schranke sei $x \in L$ mit $q(x) = d$. Dann ist $px \in pL = N \cap M = N \cap N \cap M = N \cap pL$ und somit $\lambda := (px, 0, \ldots, 0) \in \Lambda$ mit $\hat{q}(\lambda) = pq(x) = pd$. □

Beispiele: 1) Das Gitter $\mathbb{E}_8$ ist unimodular, besitzt also eine triviale Diskriminantengruppe. Insbesondere ist $p = 2$ kein Teiler von $\left|\mathbb{E}_8^\#/\mathbb{E}_8\right|$ und wir können auf die oben

beschriebene Art und Weise eine Polarisation (M, N) von $(\mathbb{E}_8, q)$ mit $q(x) = \frac{1}{2}\sum_{i=1}^{8} x_i^2$ bilden. Da M und N ebenfalls gerade und unimodulare Gitter sind, gilt $\min(\mathbb{E}_8, q) = \min(M, \frac{1}{2}q) = \min(N, \frac{1}{2}q) = 1$ und aus Lemma (2.7) folgt, dass $(\Lambda(L, M, N, k), \hat{q})$ für $k \in \{2, 3, 4, 5\}$ extremal ist. Insbesondere gilt $\min(\Lambda(L, M, N, 3), \hat{q}) = 2$ und weil das Leech-Gitter das eindeutige gerade unimodulare extremale Gitter vom Rang 24 ist ([2]), muss $(\Lambda(L, M, N, 3), \hat{q})$ isometrisch zu dem Leech-Gitter sein.

2) Sei L das Leech-Gitter und (M, N) eine Polarisation zu $p = 2$ mit $\min(L) = \min(M) = \min(N) = 2$. Aus Lemma (2.7) folgt dann $\min(\Lambda(L, M, N, k), \hat{q}) \in \{k, k+1\}$ für $k = 2, 3$ und $\min(\Lambda(L, M, N, k), \hat{q}) = 4$ für $k \geq 4$.

3) Wir müssen uns aber nicht auf die Untersuchung unimodularer Gitter beschränken, da Satz (2.4) und die beiden Konstruktionen sich auf beliebige gerade positiv definite Gitter von geradem Rang anwenden lassen. Sei e_i das i-te Standardbasiselement des $\mathbb{R}^8$ und $(\mathbb{R}^8, q)$ ein quadratischer Modul mit b_q als Standardskalarprodukt, also $q(x) = \frac{1}{2}\sum_{i=1}^{8} x_i^2$. Wir betrachten das Gitter $\mathbb{E}_6 = \langle f_1, \ldots, f_6 \rangle$ mit $f_i = e_{i+2} - e_{i+1}$ für $1 \leq i \leq 5$ und $f_6 = \frac{1}{2}(e_1 + \ldots + e_4 - e_5 - \ldots - e_8)$ in dem reellen quadratischen Vektorraum $V := (\mathbb{E}_6 \otimes \mathbb{R}, q|_{\mathbb{E}_6 \otimes \mathbb{R}})$. Das Gitter $\mathbb{E}_6$ ist gerade mit $\left|\mathbb{E}_6^{\#}/\mathbb{E}_6\right| = 3$. Die kleinste Primzahl p für die $\mathbb{E}_6/p\mathbb{E}_6$ hyperbolisch ist, zu der wir also eine Polarisation (M, N) von $\mathbb{E}_6$ konstruieren können, ist $p = 7$. Es gilt $\mathbb{E}_6/7\mathbb{E}_6 = \left\langle \bar{f}_1, \ldots, \bar{f}_6 \right\rangle$ und mit Magma ([1]) berechnen wir eine Zerlegung $\mathbb{E}_6/7\mathbb{E}_6 = A \oplus A'$ mit singulären Unterräumen A, A' (bezüglich $\bar{q}$) gegeben durch

$$A = \left\langle \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 6 \\ 5 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 6 \\ 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 5 \\ 0 \\ 4 \\ 0 \end{pmatrix} \right\rangle \quad \text{und} \quad A' = \left\langle \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 4 \\ 6 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 4 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \\ 4 \\ 0 \end{pmatrix} \right\rangle$$

bezüglich der Basis $\bar{f}_1, \ldots, \bar{f}_6$. Es gilt $\min(\mathbb{E}_6, q) = \min(M, \frac{1}{7}q) = \min(N, \frac{1}{7}q) = 1$ und Lemma (2.7) liefert uns die Abschätzung $1 \leq \min(\Lambda(\mathbb{E}_6, M, N, k), \hat{q}) \leq 7$ für $1 \leq k \leq 6$. Konstruieren wir die Gitter nun konkret mit Magma, so erhalten wir $\min(\Lambda(\mathbb{E}_6, M, N, k), \hat{q}) = 1$ für $1 \leq k \leq 5$ und $\min(\Lambda(\mathbb{E}_6, M, N, 6), \hat{q}) = 2$. Berechnen wir damit die Dichte $D(\Lambda)$, so stellt sich heraus (vgl. [3]), dass in den entsprechenden Dimensionen eine wesentlich höhere Dichte erreicht werden kann. Die Dichte eines Gitters hängt aber nur von der Ordnung der Diskriminantengruppe und dem Minimum ab und nach Satz (2.4) gilt $\Lambda^{\#}/\Lambda \cong (\mathbb{E}_6^{\#}/\mathbb{E}_6)^m$, also erhalten wir mit Konstruktion I und II stets Diskriminantengruppen gleicher Ordnung. Es stellt sich also die Frage ob wir mit der Konstruktion II Gitter mit einem größeren Minimum konstruieren können. Tatsächlich wird man beispielsweise in dem Fall $k = 5$ schnell fündig, indem

wir $\sigma_1 = \sigma_2 = \sigma_3 = id_A$ wählen und σ_4, σ_5 durch

$$\sigma_4(A_1) = A_1 + A_2, \quad \sigma_4(A_2) = A_2 + A_3, \quad \sigma_4(A_3) = A_3 + A_1,$$
$$\sigma_5(A_i) = A_1 + A_2 + A_3 \quad \text{für } 1 \leq i \leq 3$$

definieren, wobei A_i die oben angegebenen Basiselemente von A bezeichnen. Für das so konstruierte Gitter Λ gilt $\min(\Lambda) = 2$ und $\left|\Lambda^{\#}/\Lambda\right| = \left|\mathbb{E}_6^{\#}/\mathbb{E}_6\right|^5 = 3^5$. Die Dichte der dazugehörigen Kugelpackung ist dann $\left(4/\sqrt[30]{3^5}\right)^{15} \cdot \mathrm{vol}(S_{30}) \approx 0.06415 \cdot \mathrm{vol}(S_{30})$.

Literatur

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[2] W. Ebeling. *Lattices and Codes*. Springer Spektrum, 3rd edition, 2013.

[3] G.Nebe and N.J.A. Sloane. Catalogue of Lattices., September 2013. URL `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/`.

[4] T.C. Hales. A Proof of the Kepler Conjecture. *Annals of Mathematics*, 162:1065–1185, 2005.

[5] M. Kneser. *Quadratische Formen*. Springer, 2002.

[6] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes. Parts I, II. (3rd repr.).* 1985. ISBN 0-444-85193-3.

[7] C.L. Mallows and N.J.A. Sloane. An Upper Bound for Self-Dual Codes. *Information and Control*, 22:188–200, 1973.

[8] C.L. Mallows, A.M. Odlyzko, and N.J.A. Sloane. Upper Bounds for Modular Forms, Lattices, and Codes. *J. Algebra*, 36:68–76, 1975.

[9] G. Nebe. A Generalisation of Turyn's Construction of Self-Dual Codes. 2010.

[10] H.-G. Quebbemann. A Construction of Integral Lattices. *Mathematika*, 31:137–140, 1984.

[11] Shengyuan Zhang. On the nonexistence of extremal self-dual codes. *Discrete Appl. Math.*, 91(1-3):277–286, 1999.