2.3 Liftung binärer Codes

Wir besprechen eine erste -im Grunde sehr einfache- Konstruktion, die einem linearen binären Code C ein Gitter $L(C)$ zuordnet. Die wichtigsten Eigenschaften des Gitters lassen sich aus entsprechenden Eigenschaften des Codes ablesen, wie wir im folgenden Satz sehen werden.

Definition 2.3.1 (Gewöhnliche Liftung eines binären Codes) Es sei $a_1, \ldots, a_n$ eine Orthogonalbasis von V mit $\langle a_i, a_j \rangle = 2\delta_{ij}$. Definiere die *Liftung* $L(C)$ eines Codes $C \subseteq \mathbb{F}_2^n$ durch

$$L(C) := \left\{ \frac{1}{2} \sum_{i=1}^{n} x_i a_i \mid x_i \in \mathbb{Z},\ (\overline{x}_1, \ldots, \overline{x}_n) \in C \right\}$$

(wobei $\overline{x}_i = x_i + 2\mathbb{Z}$ die Restklasse von x_i modulo 2 bezeichnet).

Wenn aus dem Zusammenhang hervorgeht, welche Konstruktion gemeint ist, werden wir ein Gitter $L(C)$ auch einfach als *Codegitter* bezeichnen. Bevor wir uns den Eigenschaften von $L(C)$ zuwenden, wollen wir die Definition etwas erläutern. Zu der gewählten Basis betrachten wir die beiden Gitter

$$L_0 := \mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots + \mathbb{Z}a_n \text{ und } \frac{1}{2}L_0 \supset L_0.$$

Nach Definition ist jedes Gitter der Gestalt $L(C)$ in $\frac{1}{2}L_0$ enthalten. Wenn wir die Faktorgruppe $\frac{1}{2}L_0/L_0$ vermöge der Basis $\frac{1}{2}a_1, \ldots, \frac{1}{2}a_n$ mit $\mathbb{Z}^n/(2\mathbb{Z})^n \cong \mathbb{F}_2^n$ identifizieren, ist $L(C)$ gerade das Urbild von C unter der kanonischen Projektion $\pi : \frac{1}{2}L_0 \to \mathbb{F}_2^n$. Das Urbild eines einzelnen Codewortes $\mathbf{c} \in \mathbb{F}_2^n$ ist eine Nebenklasse $v + L_0$, also geometrisch ein verschobenes Gitter; $L(C)$ ist dementspechend eine Vereinigung von solchen Translaten von Gittern. Diese Überlegungen gelten offenbar für einen beliebigen, nicht notwendig linearen Code. Wenn C linear ist, ist $L(C)$ eine Gruppe, also ein Gitter. Wegen $C = \pi(L(C))$ gilt auch die Umkehrung. Als Vertreter für die zu einem $\mathbf{c} \in C$ gehörige Klasse nimmt man für $\mathbf{c} \neq 0$ zweckmäßigerweise den Vektor

$$v_{\mathbf{c}} := \frac{1}{2} \sum_{i=1}^{n} c_i a_i \in \tfrac{1}{2}L_0. \tag{2.3.1}$$

(Hierbei sind die Elemente $c_i \in \mathbb{F}_2$ als ganze Zahlen 0 bzw. 1 zu lesen.) Dieser Vektor hat die Quadratlänge $m \cdot \frac{1}{4} \cdot 2 = m/2$, wobei $m = \mathrm{wt}(c)$ die Zahl der Einsen, also das Hamming-Gewicht in C ist. Scharfes hinsehen zeigt, dass alle anderen Vektoren $v' = v_{\mathbf{c}} + v_0,\ v_0 \in L_0$ mindestens die gleiche (Quadrat)länge haben, also $\|v\| \leq \|v'\|$. Gleichheit kommt hier durchaus vor. Genauer gilt:

Bemerkung 2.3.2 Der Vektor $v_{\mathbf{c}}$ ist eine kürzester Vertreter für seine Nebenklasse $v_{\mathbf{c}} + L_0$. Diese Nebenklasse besitzt insgesamt $2^{\mathrm{wt}(\mathbf{c})}$ kürzeste Vektoren, nämlich die Elemente

$$\frac{1}{2}\sum_{i=1}^{n} \varepsilon_i c_i a_i \text{ mit } \varepsilon_i \in \{1, -1\}. \tag{2.3.2}$$

Wir wenden uns nun der Frage zu, welche Vektoren von $L(C)$ ganze oder sogar gerade Quadratlänge $\langle v, v\rangle$ haben. Die folgende Rechnung zeigt, dass dieses nur von der Nebenklasse abhängt. Für $v = v_{\mathbf{c}} + y \in v_{\mathbf{c}} + L_0$ gilt

$$\langle v, v\rangle = m/2 + 2\langle v_{\mathbf{c}}, y\rangle + \langle y, y\rangle \equiv m/2 \pmod{2\mathbb{Z}}. \tag{2.3.3}$$

Wenn $\mathrm{wt}(\mathbf{c}) \equiv 0 \pmod 2$ ist, haben also alle Vektoren aus der Nebenklasse zu $\mathbf{c}$ ganze Quadratlänge, und wenn $\mathbf{c} \equiv 0 \pmod 4$ ist, sogar gerade Quadratlänge.

Im folgenden Satz fassen wir die wichtigsten Eigenschaften der Gitter $L(C)$ in Abhängigkeit von Code C zusammen. Zur Bestimmung des dualen Gitters in Teil e) müssen wir an den dualen Code 2.1.9 erinnern.

Satz 2.3.3 (Das Gitter-Codes-Dictionary A)

a) Wenn C linear ist (und nur dann), ist $L(C)$ ein Gitter.

Dieses sei im folgenden erfüllt, $k = \dim C$.

b) $\det L(C) = 2^{n-2k}$

c) $L(C)$ ist ganzzahlig genau dann, wenn C selbstorthogonal*, d.h. $C \subseteq C^{\perp}$ ist.*

d) $L(C)$ ist gerade genau dann, wenn C doppelt gerade *ist, d.h.* $\mathrm{wt}(c) \equiv 0 \pmod 4$ *für alle $c \in C$.*

e) $L(C)^{\#} = L(C^{\perp})$

f) $L(C)$ ist selbstdual, $L(C) = L(C)^{\#}$ genau dann, wenn C selbstdual*, d.h. $C = C^{\perp}$ ist.*

g)

$$\begin{array}{lcl} \min L(C) = 2 & \iff & \min C \geq 4 \\ \mathrm{Min}\, L(C) = \{\pm a_i \mid i = 1, \ldots, n\} & \iff & \min C > 4 \end{array}$$

Zum Beweis ist nach den Vorbemerkungen hauptsächlich noch e) zu zeigen, woraus c) und f) unmittelbar folgen.

Als ein interessantes Beispiel für den Satz 2.3.3 betrachten wir das Gitter $L(\mathcal{H}_8)$, das aus dem Hamming-Code $\mathcal{H}_8$ entsteht. Dieses ist ganzzahlig und sogar gerade, ferner selbstdual (weil $\mathcal{H}_8$ es ist). Alle diese Eigenschaften hat auch das Wurzelgitter E_8. Wir überlegen uns nun, dass die beiden Gitter sogar isometrisch sind.

Proposition 2.3.4 *Das Gitter $E_8 = D_8^+$ ist isometrisch zu dem Gitter $L(\mathcal{H}_8)$, das durch Liftung aus dem (erweiterten) $[8,4,4]$-Hamming-Code entsteht.*

Zur Vorbereitung des Beweises machen wir uns klar, welche Gitter man überhaupt in der Gestalt $L(C)$ schreiben kann. Ausgangspunkt der Konstruktion von $L(C)$ war das Teilgitter $\mathbb{Z}a_1 \perp \mathbb{Z}a_2 \perp \ldots \perp \mathbb{Z}a_n$, also ein zu ${}^2I_n$ isometrisches Gitter. [5] Umgekehrt ist offenbar jedes Gitter L, das ein Teilgitter $L_0 \cong {}^2I_n$ enthält derart, dass $2L \subseteq L_0$ ist, isomorph zu einem Gitter $L(C)$. Der zugehörige binäre Code C ist offensichtlich wie folgt zu definieren: Wähle eine Basis $a_1, \ldots, a_n$ von L_0 mit $\langle a_i, a_j \rangle = 2\delta_{ij}$ und definiere $C = \{(\overline{x}_1, \ldots, \overline{x}_n) \mid x_i \in \mathbb{Z}\,,\ \frac{1}{2}\sum x_i a_i \in L\}$.

Es ist noch bemerkenswert, dass die Bedingung $2L \subseteq L_0$ automatisch erfüllt ist, wenn L ganzzahlig ist. Denn schreibe $v \in L$ als $v = \frac{1}{2}\sum x_i a_i$, $x_i \in \mathbb{Q}$. Dann ist $x_i = \langle v, a_i \rangle$, also $x_i \in \mathbb{Z}$, also $2v \in L_0$. Wir halten diese Überlegung in zitierfähiger Form fest:

Bemerkung 2.3.5 *Ein ganzzahliges Gitter L ist genau dann von der Form $L(C)$, für einen (selbstorthogonalen) binären Code C, wenn L ein zu ${}^2I_0$ isometrisches Teilgitter enthält.*

Beweis von 2.3.4: Man sieht sofort, dass E_8 acht paarweise orthogonale Vektoren der Quadratlänge 2 enthält. Z.B. kann man die Vektoren $\mathbf{e}_1 + \mathbf{e}_2, \mathbf{e}_1 - \mathbf{e}_2, \mathbf{e}_3 + \mathbf{e}_4, \mathbf{e}_3 - \mathbf{e}_4, \mathbf{e}_5 + \mathbf{e}_6, \mathbf{e}_5 - \mathbf{e}_6, \mathbf{e}_7 + \mathbf{e}_8, \mathbf{e}_7 - \mathbf{e}_8$ aus $D_8 \subset E_8$ nehmen, wobei die $\mathbf{e}_i$ die Standardbasis des $\mathbb{Z}^n$ bilden. Nun liefert die Bemerkung 2.3.5 einen Code $C \subseteq \mathbb{F}_2^8$ mit $L(C) \cong E_8$. Die Eigenschaften von C ergeben sich aus 2.3.3. Insbesondere ist $\dim C = 4$ nach b) und $\min C \geq 4$ (sogar $\min C = 4$) nach g). Nach 2.2.6 (Eindeutigkeit des $[8,4,4]$-Codes) folgt $C \cong \mathcal{H}_8$. Hieraus wiederum folgt $L(C) \cong L(\mathcal{H}_8)$, also $E_8 \cong L(\mathcal{H}_8)$, wie behauptet. □

[5] Als generelle Notation bedeutet der linke obere Index 2 die *Skalierung* um den Faktor 2, also die Multiplikation des Skalarpeoduktes mit 2.