6 Block-zerlegbare divisible Designs und ihre Codes

Dieses abschließende Kapitel dient der Übertragung einiger Ergebnisse dieser Arbeit auf Codes konstanten Gewichts. Das ist möglich, da eine direkte Verbindung zwischen DDs und speziellen Codes dieser Art hergestellt werden kann (s. [80]). Weitere Arbeiten zu diesem Themenbereich sind zum Beispiel [84], [24], [7], [66] und [67].

In diesem Kapitel wird zunächst eine Möglichkeit beschrieben, mit welcher zu einem beliebigen t-DD ein sogenannter *assoziierter* CW-Code erstellt werden kann. Dies ermöglicht eine Übertragung von Existenzaussagen zu t-DDs auf deren assoziierte Codes. Anschließend beschreiben wir die strukturelle Übereinstimmung von t-DDs und ihren zugehörigen Codes und nutzen den Zusammenhang der jeweiligen Automorphismengruppen. Um Aussagen zum Minimalabstand machen zu können, definieren wir diesen für Blöcke eines t-DDs, setzen ihn in Beziehung zum Minimalabstand der assoziierten Codes und nutzen strukturelle Eigenschaften der t-DDs. Schließlich werden einige Beispiele angegeben, in denen der Minimalabstand eines durch Konstruktion (A) erstellten t-DDs, bei vorgegebenem Minimalabstand des Starter-Designs, leicht berechnet werden kann.

Wir verstehen unter einem Code konstanten Gewichts folgendes:

Definition 6.0.8 Ein m-närer *Code konstanten Gewichts* (CW-Code) C der Länge n und Gewicht w ist definiert als eine Menge C mit

$$C \subseteq (\mathbb{Z}_m)^n \text{ mit } w_H(c) = w \text{ für alle } c \in C.$$

Dabei ist

$$w_H(c) := d_H(c, 0)$$

als das *Hamming-Gewicht* definiert, wobei $d_H(c, c')$ als die Anzahl der unterschiedlichen Komponenten (der *Hamming-Abstand*) von c und c' definiert ist.

Außerdem definieren wir

$$d_{min}C := \min\{d_H(c, c') \mid c, c' \in C \text{ mit } c \neq c'\}$$

als den *Minimalabstand von* C.

Der Minimalabstand ist insbesondere wegen seines Zusammenhanges zu den Fehlererkennungs- und Fehlerkorrektureigenschaften des zugehörigen Codes von Interesse (s. z.B. [81]).

6.1 *t*-divisible Designs und assoziierte CW-Codes

In [80] (s.a. [84]) wird in Verallgemeinerung von Methoden, die bei binären Codes verwendet werden, ein Konstruktionsverfahren angegeben, mit welchem ein $(s+1)$-närer Code konstanten Gewichts der Länge n, ausgehend von einem divisiblen Design erstellt wird (s.a. Konstruktion in [24], welche unabhängig von [80] entstanden ist). Dieses Verfahren wird nun skizziert dargestellt.

Sei $D = (\mathcal{P}, \mathcal{B}, S)$ ein $t-(s, k, \lambda_t)$-DD mit v Punkten und b Blöcken. Zunächst wird zu jeder Punktklasse $G_i \in S$ ein neuer Punkt O_i hinzugefügt, den wir als *idealen Punkt* bezeichnen. Nun definieren wir zu jedem Block $B \in \mathcal{B}$

$$\overline{B} := B \cup \{O_i \mid B \text{ enthält keinen Punkt aus } G_i\}.$$

Außerdem definieren wir $\overline{\mathcal{B}} := \{\overline{B} \mid B \in \mathcal{B}\}$, $\overline{\mathcal{P}} := \mathcal{P} \cup \{O_i \mid i = 1, \ldots, n\}$, $\overline{S}$ als Menge der erweiterten Punktklassen und nennen $\overline{D} := (\overline{\mathcal{P}}, \overline{\mathcal{B}}, \overline{S})$ den *Abschluss* von D.

Mit geeigneter Nummerierung der Punktklassen und der darin enthaltenen Punkte, wobei den idealen Punkten jeweils die Nummer 0 zugeordnet wird, erhalten wir mit $\mathbb{Z}_{n+1}^* := \mathbb{Z}_{n+1} \setminus \{0\}$ o.B.d.A.

$$\mathcal{P} = \mathbb{Z}_{n+1}^* \times \mathbb{Z}_{s+1}^* \quad \text{und} \quad \overline{\mathcal{P}} = \mathbb{Z}_{n+1}^* \times \mathbb{Z}_{s+1}.$$

Jeder Block $B \in \mathcal{B}$ kann in Form von $B = \{(i_1, j_{i_1}), \ldots, (i_k, j_{i_k})\}$ und der zugehörige Block $\overline{B} \in \overline{\mathcal{B}}$ als $\{(u, j_u) \mid u = 1, \ldots, n\}$, wobei $(u, j_u) = (u, 0)$ mit $u \notin \{i_1, \ldots, i_k\}$ gilt, dargestellt werden. Nun definieren wir $c(B) = c(\overline{B}) := j_1 j_2 \ldots j_n$ und nennen $C(D) := \{c(B) \mid B \in \mathcal{B}\}$ den mit dem divisiblen Design D assoziierten Code.

Ein solcher Code besitzt bestimmte Eigenschaften und lässt sich bis auf Isomorphie eindeutig charkterisieren:

Bemerkung 6.1.1 ([84]) Der Code $C(D)$ eines $t-(s, k, \lambda_t)$-DDs D mit m Punktklassen besitzt folgende Eigenschaften:

(i) $C(D) \subseteq \mathbb{Z}_{s+1}^m$;

(ii) $C(D)$ ist ein CW-Code mit $w = k$;

(iii) zu je t verschiedenen Positionen $i_1, \ldots, i_t$ aus $\{1, \ldots, m\}$ und Elementen $j_1, \ldots, j_t$ aus $\{1, \ldots, s\}$ gibt es genau λ_t Codewörter $c \in C(D)$ mit den Einträgen j_u an den Positionen i_u für $u = 1, \ldots, t$.

Umgekehrt gilt ([84]):
Ist C ein Code mit den Eigenschaften (i), (ii) und (iii), so existiert bis auf Isomorphie genau ein $t-(s,k,\lambda_t)$-divisibles Design D mit m Punktklassen, für welches $C = C(D)$ gilt.

Bemerkung 6.1.2 Ist D ein $t-(1,k,\lambda_t)$-DD, also ein t-Design, erhalten wir mit der obigen Konstruktion einen binären CW-Code.

Wir haben uns in dieser Arbeit viel mit divisiblen Unterdesigns divisibler Designs beschäftigt, daher ist es naheliegend, den Abschluss eines t-DD bezüglich einer größeren Punktklassenmenge zu definieren.

Definition 6.1.3 Sei $D = (\mathcal{P}, \mathcal{B}, S)$ ein divisibles Unterdesign eines t-divisiblen Designs $\tilde{D} = (\tilde{\mathcal{P}}, \tilde{\mathcal{B}}, \tilde{S})$ und sei $\overline{D}$ der Abschluss von D. Wir fügen zu jeder Punktklasse $G_i \in \tilde{S}$, für die $G_i \cap G_j = \emptyset$ mit $G_j \in S$ gilt, einen *idealen Punkt* $\mathcal{O}_i$ hinzu, bezeichnen die Menge dieser Punkte als $\mathcal{O}$ und die Menge dieser erweiterten Punktklassen als $\tilde{S}^{\mathcal{O}}$. Nun definieren wir:

$$\overline{\mathcal{P}}^{\tilde{S}} := \overline{\mathcal{P}} \cup \mathcal{O}, \quad \overline{B}^{\tilde{S}} := \overline{B} \cup \mathcal{O}, \quad \overline{\mathcal{B}}^{\tilde{S}} := \{\overline{B}^{\tilde{S}} \mid B \in \mathcal{B}\} \text{ und } \overline{S}^{\tilde{S}} := \overline{S} \cup \tilde{S}^{\mathcal{O}}.$$

Wir nennen $\overline{D}^{\tilde{S}} := (\overline{\mathcal{P}}^{\tilde{S}}, \overline{\mathcal{B}}^{\tilde{S}}, \overline{S}^{\tilde{S}})$ den *Abschluss von D bezüglich $\tilde{S}$.*

Völlig analog zu oben konstruiert man nun einen zu D *assoziierten CW-Code bezüglich $\tilde{S}$*, den wir als $C(D^{\tilde{S}})$ bezeichnen.
Man beachte, dass sich $C(D^{\tilde{S}})$ durch geeignete Verkürzungen, also Entfernungen von Komponenten in jedem Codewort an jeweils denselben Stellen, in $C(D)$ umwandeln lässt.

6.1.1 Existenz von CW-Codes

Als direkte Folgerung aus Bemerkung 6.1.1 und Satz 3.2.7 erhalten wir:

Proposition 6.1.4 *Sei $C_0 \subseteq (\mathbb{Z}_{s+1}^{vs^{-1}})$ ein $(s+1)$-närer CW-Code der Länge vs^{-1} und vom Gewicht k, der die Eigenschaften (i), (ii) und (iii) aus 6.1.1 erfüllt und b Codewörter enthält. Dann existiert zu jedem $i \in \mathbb{N}$ ein (sq^i+1)-närer CW-Code $C_i \subseteq (\mathbb{Z}_{sq^i+1}^{vs^{-1}})$ derselben Länge und desselben Gewichts, der die Eigenschaften (i) bis (iii) analog erfüllt und $b \cdot q^{i(n-d)}$ Codewörter enthält. Dabei sind $q, n, d \in \mathbb{N}$ geeignet gewählt*[57]*, das heißt, q ist Primzahlpotenz und es gilt $(q^{n+1}-1)(q-1)^{-1} \geq v$.*

Analog zu Korollar 3.2.9 erhalten wir auch hier wegen Bemerkung 3.2.8:

[57] Dabei ergibt sich „d“ aus der Konstruktion zu C_i, s. S. 71 und beschreibt *nicht* den Minimalabstand von C_i, wie man vielleicht fälschlicherweise vermuten könnte.

Korollar 6.1.5 *Sei $C_0 \subseteq (\mathbb{Z}_{s+1}^{vs^{-1}})$ ein $(s+1)$-närer CW-Code der Länge vs^{-1} und vom Gewicht k, der die Eigenschaften (i), (ii) und (iii) aus 6.1.1 erfüllt und b Codewörter enthält. Dann existiert zu jedem $i \in \mathbb{N}$ und jeder Primzahlpotenz q mit $q \geq v-1$ ein (sq^i+1)-närer CW-Code $C_i \subseteq (\mathbb{Z}_{sq^i+1}^{vs^{-1}})$ derselben Länge und desselben Gewichts, der die Eigenschaften (i) bis (iii) analog erfüllt und $b \cdot q^{2i}$ Codewörter enthält.*

6.1.2 Zerlegbarkeit von CW-Codes

Da wir mit der im letzten Abschnitt beschriebenen Konstruktion zu jedem beliebigen t-DD einen zugehörigen CW-Code erhalten, wobei jedem Block genau ein Codewort zugeordnet ist, lässt sich die Block-Zerlegbarkeit eines t-DDs direkt auf den zugehörigen CW-Code $C(D)$ übertragen.

Theorem 6.1.6 *Sei $\tilde{D} = (\tilde{\mathcal{P}}, \tilde{\mathcal{B}}, \tilde{S})$ ein block-zerlegbares t-DD mit m Punktklassen und inneren t_i-DDs $D_i = (\tilde{\mathcal{P}}_i, \tilde{\mathcal{B}}_i, \tilde{S}_i)$, $i \in N \subset \mathbb{N}$. Dann existiert ein CW-Code $C(\tilde{D})$, dessen Codewörter eine Partition zulassen, so dass jeder Teil dieser Partition isomorph zu einem Code $C(D_i^{\tilde{S}})$ ist, das heißt, dass sich $C(\tilde{D})$ in kleinere CW-Codes zerlegen lässt, die selbst jeweils die Eigenschaften aus Bemerkung 6.1.1 erfüllen, wobei Bedingung (iii) jeweils für t_i, $i \in N$ gilt.*

Beweis: Seien $\tilde{D}$ und D_i, $i \in N$ wie oben gegeben. Nach Konstruktion existiert eine Bijektion zwischen Blöcken und Codewörtern, weshalb sich die Partition der Blockmenge von D auf die Menge der Codewörter von $C(D)$ übertragen lässt.

Die Konstruktion von $C(\tilde{D})$ beinhaltet die Erstellung von Teilcodes C_i, die bei geeigneter Nummerierung jeweils mit $C(D_i^{\tilde{S}})$, $i \in N$ übereinstimmen. □

Bei einem solchen zerlegbaren CW-Code $C(\tilde{D})$ bezeichnen wir, analog zu block-zerlegbaren t-DDs, Teilcodes $C(D_i^{\tilde{S}})$, die zu inneren Designs D_i (bezüglich $\tilde{S}$) assoziiert sind, als *innere Codes von* $C(\tilde{D})$ und bemerken, dass eine Isomorphie zwischen zwei inneren Designs von $\tilde{D}$ eine ebensolche auch bei den dazu (bezüglich $\tilde{S}$) assoziierten inneren Codes induziert (s. nächster Abschnitt).

6.1.3 Automorphismengruppen

Die innere Strukturierung eines DDs $\tilde{D}$ induziert eine solche also auch auf dem assoziierten CW-Code $C(\tilde{D})$.

In [84] zeigen Schulz und Spera, dass es auch zwischen den Automorphismengruppen von DDs und den Automorphismengruppen der dazu assoziierten Codes eine enge Verbindung gibt (s.u. Satz 6.1.8). Dies lässt uns Eigenschaften einer dualen Translationsgruppe auch bei den zugehörigen CW-Codes nutzen und wir erhalten eine Möglichkeit, bei speziellen CW-Codes, die aus paarweise isomorphen inneren Codes bestehen, auf sehr einfache Art einen binären CW-Code zu bestimmen, der zu den inneren Codes isomorph ist. Dabei gehen wir wie folgt vor:

Wir ersetzen bei jedem Codewort an jeder Position, deren Eintrag ungleich Null ist, diesen durch eine Eins. Die Menge (nicht Multimenge) dieser Codewörter bezeichnen wir als $C(\tilde{D})_{(0,1)}$. Wir werden in Lemma 6.1.9 zeigen, dass $C(\tilde{D})_{(0,1)}$ zu den inneren Codes von $C(\tilde{D})$ isomorph ist.

Zuerst wird jedoch definiert, was man unter einem Automorphismus einer Menge von Wörtern und was man unter der Automorphismengruppe eines Codes versteht. Außerdem geben wir den für diesen Abschnitt entscheidenden Satz aus [84] an.

Definition 6.1.7 Ein *Automorphismus* der Menge $\mathcal{A}^m$ aller Wörter der Länge m über dem Alphabet $\mathcal{A}$ ist als eine Abbildung definiert, die aus m Permutationen $\alpha_1, \ldots, \alpha_m$ besteht, wobei jeweils α_i eine Permutation des Alphabets $\mathcal{A}$ in der i-ten Komponente ist, gefolgt von einer Permutation α_0 der Komponenten von $\mathcal{A}^m$.
Bei einem Code $C \subseteq \mathcal{A}^m$ besteht die *Automorphismengruppe* $\mathrm{Aut}C$ aus allen Automorphismen $\alpha \in \mathrm{Aut}\mathcal{A}^m$ für die $\alpha(C) = C$ gilt.

Theorem 6.1.8 *([84], Th. (3.1)) Sei $\tilde{D}$ ein divisibles Design und $C = C(\tilde{D})$ der zu $\tilde{D}$ assoziierte CW-Code. Dann induziert $\mathrm{Aut}\tilde{D}$ treu eine Gruppe H von Automorphismen des Codes C. Entweder gilt $H = \mathrm{Aut}C$ und folglich $\mathrm{Aut}\tilde{D} \cong \mathrm{Aut}C$ oder $\tilde{D}$ ist ein 2-Design mit $v = 2k$ und es gilt $[\mathrm{Aut}C : H] = 2$.*

Den Beweis hierzu findet man in [84].

Lemma 6.1.9 *Sei $\tilde{D}$ ein block-zerlegbares t-DD mit einem t-Design D als Wurzel und Gruppe T, wobei T duale Translationsgruppe von $\tilde{D}$ ist und sei $C(\tilde{D})$ der dazu assoziierte $(s+1)$-näre CW-Code. Dann ist der zugehörige binäre Code $C(\tilde{D})_{(0,1)}$ isomorph zu dem mit D bezüglich $\tilde{S}$ assoziierten Code $C(D^{\tilde{S}})$, und bei geeigneter Nummerierung gilt $C(D^{\tilde{S}}) = C(\tilde{D})_{(0,1)}$.*

Beweis: Im Beweis zu Satz 6.1.8 wird in [84] gezeigt, dass jedes $\gamma \in \mathrm{Aut}\tilde{D}$ ein $\hat{\gamma} \in \mathrm{Aut}C$ folgender Form induziert: $\hat{\gamma} = \gamma_0 \circ (\gamma_1, \ldots, \gamma_m)$, wobei $\gamma_0 \in S_m$ und $\gamma_i : \mathbb{Z}_{s+1} \to \mathbb{Z}_{s+1}$ eine Bijektion ist, welche die Null fest lässt, für alle

$i = 1, \ldots, m$. $\hat{\gamma}$ ist Bijektion von $\mathbb{Z}_{s+1}^m$ auf sich und (z.B. nach [42]) ein Element des Kranzproduktes $S_m \wr S_{s+1}$.

Man beachte, dass γ_0 einer Permutation der Punktklassen entspricht. Besitzt ein divisibles Design $\tilde{D}$ einen Automorphismus γ, der die Punktklassen fest lässt, wie es beispielsweise die Elemente der dualen Translationsgruppe tun, dann gilt $\gamma_0 = \mathrm{id}$ für den zugehörigen Automorphismus $\hat{\gamma} \in \mathrm{Aut}C$. Die Stellen eines Codewortes werden dann durch $\hat{\gamma}$ also nicht permutiert. Das bedeutet jedoch, dass ein Eintrag mit Null jeweils konstant bleibt, da jedes γ_i (mit $i = 1, \ldots, m$) die Null nach Voraussetzung fest lässt.

Damit enthält der Orbit eines Codewortes unter Automorphismen $\hat{\gamma} \in \mathrm{Aut}C$, die von Elementen der dualen Translationsgruppe des zugehörigen DDs induziert sind, ausschließlich Codewörter, die an denselben Positionen eine Null enthalten.

Da das zugehörige DD $\tilde{D}$ zusätzlich ein t-Design D als Wurzel und die duale Translationsgruppe als ihre Gruppe besitzt, können wir schließen, dass die Wurzel aus jeder Punktklasse von $\tilde{D}$ genau ein Element enthält, so dass bei geeigenter Nummerierung der zur Wurzel bezüglich $\tilde{S}$ assoziierte Code $C(D^{\tilde{S}})$ binär ist und dass jedes Codewort im Orbit eines Worts von $C(D^{\tilde{S}})$ unter der von T induzierten Automorphismengruppe liegt, weshalb $C(D^{\tilde{S}}) = C(\tilde{D})_{(0,1)}$ gilt.[58] □

6.1.4 Der Minimalabstand

Abschließend widmen wir uns noch ein wenig der Untersuchung des Minimalabstands von Codes, die zu einem t-DD assoziiert sind. Bekanntlich ist der Minimalabstand äußerst bedeutsam für die Fehlererkennungs- und Fehlerkorrektureigenschaften eines Codes [81].

Da die Codewörter eines solchen Codes durch die Blöcke des zugehörigen t-DDs induziert sind, beginnen wir mit der Definition des Abstands zweier Blöcke eines t-DDs. Wir halten fest, dass sich zwei Blöcke in zweierlei Hinsicht unterscheiden können: 1. Es gibt Punktklassen, aus der beide Blöcke jeweils ein Element enthalten, aber diese Elemente sind nicht gleich. 2. Es gibt Punktklassen, aus denen nur einer der Blöcke ein Element enthält.

Diese Unterscheidung wird hilfreich sein, wenn wir den Abstand zweier Blöcke des zugehörigen Abschlusses und damit auch des assoziierten Codes beschreiben.

[58] Bei „nicht-geeigneter“ Nummerierung erhalten wir Isomorphie.

Definition 6.1.10 Sei $D = (\mathcal{P}, \mathcal{B}, S)$ ein $t-(s,k,\lambda_t)$-DD mit Punktklassen $G_i, i \in \{1,\ldots,m\} =: M$. Wir definieren für alle $B, B' \in \mathcal{B}$ mit $B \neq B'$ als *Abstand*

$$\delta_{(B,B')} := k - |B \cap B'| = |\alpha_{(B,B')}| + |\beta_{(B,B')}|,$$

wobei

$$\alpha_{(B,B')} := \{(P,P') \in B \times B' \mid P \neq P' \wedge \exists i \in M : P, P' \in G_i\}$$

und

$$\beta_{(B,B')} := \{P \in B \mid \exists i \in M : (P \in G_i \wedge G_i \cap B' = \emptyset)\}.$$

Wir definieren

$$\delta_{min}(D) := \min\{\delta_{(B,B')} \mid B, B' \in \mathcal{B} \text{ mit } B \neq B'\}$$

als den *Minimalabstand von* D.

Bemerkung 6.1.11 Es gilt natürlich $\delta_{(B,B')} = \delta_{(B',B)}$ für alle $B, B' \in \mathcal{B}$. Wegen $\alpha_{(B,B')} = \alpha_{(B',B)}$ muss daher $|\beta_{(B,B')}| = |\beta_{(B',B)}|$ gelten.

Entsprechend zu obiger Definition 6.1.10 definieren wir den Abstand zweier Blöcke des Abschlusses von D.

Definition 6.1.12 Sei $\overline{D} := (\overline{\mathcal{P}}, \overline{\mathcal{B}}, \overline{S})$ der Abschluss von D, wobei $|\overline{S}| = m$ $(m \in \mathbb{N})$ gilt. Wir definieren für alle $\overline{B}, \overline{B'} \in \overline{\mathcal{B}}$ mit $\overline{B} \neq \overline{B'}$ als *Abstand*

$$d_{(\overline{B},\overline{B'})} := m - |B \cap B'| - |\gamma_{(\overline{B},\overline{B'})}| = |\overline{\alpha}_{(\overline{B},\overline{B'})}| + |\overline{\beta}_{(B,B')}|,$$

wobei

$$\overline{\alpha}_{(\overline{B},\overline{B'})} := \{(P,P') \in \overline{B} \times \overline{B'} \mid P \neq P' \wedge \exists i \in M : P, P' \in \overline{G_i} \setminus \{\mathcal{O}_i\}\},$$

$$\overline{\beta}_{(\overline{B},\overline{B'})} := \{P \in \overline{B} \mid \exists i \in M : (P \in \overline{G_i} \setminus \{\mathcal{O}_i\} \wedge \mathcal{O}_i \in \overline{B'})\} \,\dot\cup\, \{P' \in \overline{B'} \mid \exists i \in M : (P' \in \overline{G_i} \setminus \{\mathcal{O}_i\} \wedge \mathcal{O}_i \in \overline{B})\},$$

$$\gamma_{(\overline{B},\overline{B'})} := \{G_i \in S \mid B \cap G_i = \emptyset = B' \cap G_i\}.$$

Außerdem definieren wir

$$d_{min}(\overline{D}) := \min\{d_{(\overline{B},\overline{B'})} \mid \overline{B}, \overline{B'} \in \overline{\mathcal{B}} \text{ mit } \overline{B} \neq \overline{B'}\}$$

als den *Minimalabstand von* $\overline{D}$.

Bemerkung 6.1.13 (a) Es gilt $\overline{\alpha}_{(\overline{B},\overline{B'})} = \alpha_{(B,B')}$, für alle $\overline{B}, \overline{B'} \in \overline{\mathcal{B}}$ mit $\overline{B} \neq \overline{B'}$, da in $\overline{\alpha}_{(\overline{B},\overline{B'})}$ kein idealer Punkt vorkommt.

(b) Es gilt $|\overline{\beta}_{(\overline{B},\overline{B'})}| = 2 \cdot |\beta_{(B,B')}|$ für alle $\overline{B}, \overline{B'} \in \overline{\mathcal{B}}$ mit $\overline{B} \neq \overline{B'}$, nach Konstruktion und Bemerkung 6.1.11.

Mit Definition 6.1.12 und Bemerkung 6.1.13 erhalten wir folgendes Lemma:

Lemma 6.1.14 *Sei D ein t-DD und $\overline{D}$ sein Abschluss, dann gilt mit obigen Bezeichnungen:*

$$d_{(\overline{B},\overline{B'})} = |\alpha_{(B,B')}| + 2 \cdot |\beta_{(B,B')}|$$

für alle $\overline{B}, \overline{B'} \in \overline{\mathcal{B}}$ mit $\overline{B} \neq \overline{B'}$.

Lemma 6.1.15 *Sei D ein t-DD und $\overline{D}$ sein Abschluss, dann gilt*

$$d_{min}(\overline{D}) \geq \delta_{min}(D).$$

Beweis:
Wegen Lemma 6.1.14 gilt für alle Blöcke B, B' $(B \neq B')$ aus D:
$d_{(\overline{B},\overline{B'})} = |\alpha_{(B,B')}| + 2 \cdot |\beta_{(B,B')}| \geq |\alpha_{(B,B')}| + |\beta_{(B,B')}| \geq \delta_{min}(D)$. □

Durch Lemma 6.1.14 erhalten wir auch eine Beschreibung des Abstandes zweier Codewörter, was durch das nächste Lemma begründet ist.

Lemma 6.1.16 *Seien D ein t-DD, $\overline{D}$ sein Abschluss und $C(D)$ der zugehörige CW-Code, dann gilt für alle $B, B' \in \mathcal{B}$ mit $B \neq B'$:*

$$d_H(c(B), c(B')) = d_{(\overline{B},\overline{B'})}.$$

Beweis:
Seien $B, B' \in \mathcal{B}$ mit $B \neq B'$ beliebig gegeben, wobei $\overline{B} = \{(u, j_u) \mid u = 1, \ldots, m\}$ und $\overline{B'} = \{(u, l_u) \mid u = 1, \ldots, m\}$ und somit $C(B) = j_1 j_2 \ldots j_m$ und $C(B') = l_1 l_2 \ldots l_m$. Man sieht sofort, dass unterschiedliche Einträge $j_i \neq l_i$ $(i \in \{1, \ldots, m\})$ in $\overline{B}$ und $\overline{B'}$ zu verschiedenen Komponenten an Position i von $C(B)$ und $C(B')$ führen. □

Also folgt zusammen mit Lemma 6.1.14:

Lemma 6.1.17 *Sei $C(D)$ ein zu einem t-DD D assoziierter CW-Code, dann gilt mit den Bezeichnungen von oben:*

$$d_H(c(B), c(B')) = |\alpha_{(B,B')}| + 2 \cdot |\beta_{(B,B')}|$$

für alle Codewörter $c(B), c(B') \in C(D)$ mit $c(B) \neq c(B')$.

6.1.5 Der Minimalabstand spezieller *t*-DDs und ihrer Codes

Wir untersuchen nun den Minimalabstand eines CW-Codes, der zu einem t-DD assoziiert ist, welches unter anderem uns bereits gut bekannte Eigenschaften besitzt, nämlich (fast)-block-zerlegbar mit einer Wurzel D und Gruppe T ist, wobei die Wurzel nun einen vorgegebenen Minimalabstand d besitzen soll. Nach Lemma 6.1.17 reicht es, die Blöcke eines solchen DDs genauer zu betrachten.

Lemma 6.1.18 *Sei $\tilde{D} = (\tilde{\mathcal{P}}, \tilde{\mathcal{B}}, \tilde{S})$ ein (fast)-block-zerlegbares t-DD mit Wurzel $D = (\mathcal{P}, \mathcal{B}, S)$ und Gruppe T, wobei T duale Translationsgruppe von $\tilde{D}$ ist und die Punktmenge $\mathcal{P}$ der Wurzel aus jedem Orbit von $\mathcal{P}$ unter T genau ein Element enthält.*[59] *Dann gilt: Besitzt D einen Minimalabstand von d ($d \in \mathbb{N}$), dann*

(a) gilt dies für alle inneren Desings von $\tilde{D}$ ebenfalls und

(b) es gilt

$$d_{min}(\tilde{D}) = \min \{ \min_{\substack{B \in \mathcal{B}, \\ t \in T}} |\alpha_{(B,B^t)}| \ , \ d \}.$$

Beweis: Teil (a) folgt sofort wegen der Isomorphie der inneren Designs zur Wurzel D.

Für Teil (b) müssen wir daher nur noch den Abstand von Blöcken aus $\tilde{D}$ untersuchen, die in unterschiedlichen inneren Designs liegen. Dazu betrachten wir zunächst den Abstand zwischen Blöcken, die im selben Orbit unter T liegen.

Seien $B, B' \in \tilde{\mathcal{B}}$ mit $B \neq B'$, wobei es ein $t \in T$ gibt, für das $B^t = B'$ gilt. Da T die Punktklassen fest lässt, gilt für alle $t \in T$: $\beta_{(B,B^t)} = \emptyset$ und folglich

$$d_{(B,B^t)} = |\alpha_{(B,B^t)}|,$$

wobei die zweite Bedingung in der Definition von $\alpha_{(B,B^t)}$ (s. Definition 6.1.10) immer erfüllt ist, so dass diese Menge auch wie folgt beschrieben werden kann:

$$\alpha_{(B,B^t)} = \{(P, P^t) \in B \times B^t \mid P \neq P^t\}.$$

Der Abstand zweier solcher Blöcke beträgt mindestens

$$\min_{(B \in \tilde{\mathcal{B}}, t \in T)} |\alpha_{(B,B^t)}|.$$

Seien nun $B, B' \in \tilde{\mathcal{B}}$ mit $B \neq B'$ zwei Blöcke, die nicht im selben Orbit von $\mathcal{B}$ unter T liegen. Nach Voraussetzung ist D Wurzel und damit gibt es

[59] Da D Wurzel ist, gilt $\tilde{\mathcal{P}} = \mathcal{P}^T$. Ist $\tilde{D}$ beispielsweise durch Konstruktion (A) entstanden, so enthält $\mathcal{P}$ genau ein Element aus jedem Orbit.

zwei unterschiedliche Blöcke $B_{\mathcal{O}}, B'_{\mathcal{O}} \in \mathcal{B}$ und $t, t' \in T$, so dass $B = B_{\mathcal{O}}^t$ und $B' = B_{\mathcal{O}}'^{t'}$ gilt. Wir wissen $d_{(B_{\mathcal{O}}, B'_{\mathcal{O}})} \geq d$. Da sich die Punkte von D nach Voraussetzung in paarweise verschiedenen Orbits unter T befinden, gibt es folglich mindestens d Orbits unter T, in denen ein Punkt aus $B_{\mathcal{O}}$, aber keiner aus $B'_{\mathcal{O}}$ enthalten ist[60], was daher auch für $B = B_{\mathcal{O}}^t$ und $B' = B_{\mathcal{O}}'^{t'}$ gilt. Also erhalten wir $d_{(B,B')} \geq d$ und haben insgesamt das Lemma bewiesen. □

Korollar 6.1.19 *Sei $C(\tilde{D})$ ein zu einem t-DD $\tilde{D}$ assoziierter CW-Code, wobei $\tilde{D}$ die in Lemma 6.1.18 angegebenen Eigenschaften sowie eine Wurzel mit Minimalabstand d ($d \in \mathbb{N}$) besitzt. Dann gilt mit den obigen Bezeichnungen:*[61]

$$d_{min}(C(\tilde{D})) \geq \min \{ \min_{\substack{B \in \mathcal{B}, \\ t \in T}} |\alpha_{(B,B^t)}| \ , \ d \}.$$

Beweis: Folgt nach Lemmata 6.1.16, 6.1.15 und 6.1.18. □

6.1.6 Der Minimalabstand und Konstruktion (A)

Ein $t-(s,k,\lambda_t)$-DD, welches mit Konstruktion (A) erstellt wurde (s.a. Bemerkung 3.2.20), erfüllt alle Voraussetzungen von Lemma 6.1.18 (mit 3.2.11 und 5.0.6).

Besitzt das Starter-Design einen Minimalabstand d, dann gelten demnach Bedingungen (a) und (b) aus Lemma 6.1.18. Bei geeigneter Einbettung des Starter-Designs lässt sich $\min_{(B \in \tilde{\mathcal{B}}, t \in T)} |\alpha_{(B,B^t)}|$ leicht bestimmen.
Hierzu einige Beispiele:

- Einbettung des Starter-Designs in eine projektive Gerade ergibt $\min_{(B \in \tilde{\mathcal{B}}, t \in T)} |\alpha_{(B,B^t)}| = k-1$, da maximal Punkte (affine Geraden) einer einzigen Parallelenklasse das Zentrum einer Translation als idealen Punkt haben können und die Blöcke jeweils transversale Punktmengen sind, also davon maximal ein Punkt unter einer Translation fest bleiben kann.

- In Beispiel 2 (s. Abschnitt 3.1.2 oder auch das Beispiel auf Seite 83) werden maximal zwei Punkte (affine Ebenen) eines Blockes durch eine Translation gemeinsam festgelassen (man beachte, je drei Punkte schneiden sich genau in einem affinen Punkt), also gilt $\min_{(B \in \tilde{\mathcal{B}}, t \in T)} |\alpha_{(B,B^t)}| = k-2$.

[60] Ist D ein t-Design, so entspricht jeder Orbit von $\mathcal{P}$ unter T genau einer Punktklasse und es gilt in diesem Fall $|\alpha_{(B_{\mathcal{O}}, B'_{\mathcal{O}})}| = 0$ und $|\beta_{(B_{\mathcal{O}}, B'_{\mathcal{O}})}| \geq d$.

[61] Man beachte, dass die Menge $\alpha_{(B,B')}$ mit $B, B' \in \tilde{B}$ nur für $B \neq B'$ definiert ist!

- In Beispiel 3, Satz 3.1.17, Teil (i) (s. Abschnitt 3.1.3) werden ebenfalls maximal 2 Punkte (3-dimensionale affine Räume) eines Blockes durch eine Translation festgelassen, da der Schnitt von drei Punkten eines Blockes dem Schnitt aller Punkte dieses Blockes entspricht, weshalb eine Translation, die diese drei Punkte gemeinsam fest lässt, den ganzen Block fixieren würde. Auch in diesem Beispiel gilt daher $\min_{(B\in\tilde{\mathcal{B}},t\in T)} |\alpha_{(B,B^t)}| = k-2$.

  Wir wissen hier sogar noch mehr: Da das divisible Design 3-balanciert und der Index $\lambda_3 = 1$ ist, sind zwei Blöcke, die in mehr als zwei Punkten übereinstimmen, gleich. Daraus ergibt sich insgesamt ein Mindestabstand größer oder gleich $k-2$.

Dies kann man verallgemeinert für jedes t-DD D mit Index $\lambda_t = 1$ festhalten: $d_{min}(D) \geq k-t+1$ (s.a. [84], (2.2.5 (3))).

Dieses Kapitel zusammenfassend, können wir feststellen, dass die Block-Zerlegbarkeit von t-DDs eine Zerlegbarkeit der jeweils assoziierten CW-Codes bedingt und dass sich auch weitere strukturelle Besonderheiten, wie beispielsweise das Vorhandensein einer Wurzel, bei den zugehörigen Codes auswirken.

Mit Konstruktion (A) haben wir ein Werkzeug, mit dem (indirekt) nicht nur Serien von CW-Codes erstellt werden können, sondern auch zerlegbare Codes, bei denen man sehr leicht die inneren Codes (bis auf Isomorphie) bestimmen kann. Außerdem ist es unter Umständen möglich, den Minimalabstand eines Codes während der Konstruktion des zugehörigen t-divisiblen Designs gezielt zu beeinflussen.