HAMBURGER BEITRÄGE
ZUR MATHEMATIK

Heft 180

Extremale Mengen in endlichen metrischen Räumen - ein grundlegender Überblick

Jörn Quistorff, Hamburg

Juni 2003

Extremale Mengen in endlichen metrischen Räumen - ein grundlegender Überblick

Jörn Quistorff
E-Mail: joern.quistorff@hamburg.de

21. Juni 2003

Inhaltsverzeichnis

Vorwort

In der kombinatorischen Codierungstheorie werden die beiden folgenden klassischen Probleme diskutiert. Beim Packungsproblem sucht man die größte Kardinalität eines q-nären Codes der Länge n, dessen Minimaldistanz den Wert d nicht unterschreitet, beim Überdeckungsproblem sucht man die kleinste Kardinalität eines e-überdeckenden, q-nären Codes der Länge n. Beide Probleme können in jedem Sequenzraum aufgeworfen werden. Am häufigsten tritt dabei der Hamming-Raum auf, d.h. das n-fache cartesische Produkt K^n eines endlichen, q-elementigen Alphabets K, versehen mit der Hamming-Metrik d_H. Um analoge Probleme auch für andere Mengen und Metriken diskutieren zu können, wird in diesem Beitrag der allgemeinere Begriff des endlichen metrischen Raumes zu Grunde gelegt. Zur simultanen Betrachtung endlicher und ausgewählter unendlicher, metrischer Räume vgl. man hingegen Levenshtein [34].

Ist ein endlicher metrischer Raum, wie beispielsweise der Hamming-Raum, distanzregulär, so induziert seine Metrik ein Association Scheme, vgl. etwa Delsarte [21], MacWilliams/Sloane [42], van Lint/Wilson [38], Camion [15], Solé [56], Brouwer/Cohen/Neumaier [11]. Da diese Eigenschaft jedoch in einigen interessanten endlichen metrischen Räumen nicht erfüllt ist, wird in diesem Beitrag die Distanzregularität nicht zwingend gefordert.

Eine Motivation für die zu behandelnden Fragestellungen erfolgt in Abschnitt 1 durch elementare Probleme auf Schachbrettern und ihre Verallgemeinerungen. Hierdurch wird der etwas technischere, codierungstheoretische Zugang zunächst vermieden. In Abschnitt 2 werden die Grundlagen bereitgestellt, in Abschnitt 3 der Sequenzraum mit den wichtigsten Beispielen für endliche metrische Räume vorgestellt. In Abschnitt 4 werden Anwendungen dieser Räume diskutiert: Neben den bereits erwähnten Schachbrettproblemen, die in abstrakterer Weise vom graphentheoretischen Standpunkt wieder aufgegriffen werden, folgen Anwendungen für fehlerkorrigierende Codes, Garantiesysteme und Quasigruppen. Der Abschnitt 5 erörtert die Abschätzung extremaler Kardinalitäten. Die abschließenden Abschnitte 6 und 7 befassen sich mit ausgezeichneten Mengen und verweisen auf Tabellen mit oberen und unteren Schranken.

1 Motivation

Man betrachte ein Schachbrett mit seinen $8 \cdot 8 = 64$ Feldern, die mit

$$\{(0,0),(0,1),...,(0,7),(1,0),...,(1,7),...,(7,0),...,(7,7)\}$$

bezeichnet seien. Abkürzend verwendet man die Bezeichnung $K^2 = K \times K$ mit $K = \{0,1,...,7\}$.

Ein Turm stehe auf $(v_1, v_2) \in K^2$. Welche Felder dominiert er, d.h. welche Felder kann er neben seinem aktuellen Standort innerhalb eines Zuges erreichen? Dies sind alle Felder der selben Spalte, d.h. (w_1, w_2) mit $w_1 = v_1$, und der selben Zeile, d.h. (w_1, w_2) mit $w_2 = v_2$, also insgesamt $1 + 2 \cdot 7 = 15$ Felder.

Zur Mathematisierung definiere man einen Abstand zwischen zwei Feldern $v := (v_1, v_2)$ und $w := (w_1, w_2)$ durch $d(v,w) := |\{x \in \{1,2\} \mid v_x \neq w_x\}|$. Dann gilt $\forall v, w, z \in K^2$:

(i) (Definitheit) $d(v,w) \geq 0$ und $(d(v,w) = 0 \Leftrightarrow v = w)$.

(ii) (Symmetrie) $d(v,w) = d(w,v)$.

(iii) (Dreiecksungleichung) $d(v,w) \leq d(v,z) + d(z,w)$.

Damit ist $d : K^2 \times K^2 \to \mathbf{R}, (v,w) \mapsto d(v,w)$ eine Metrik und (K^2, d) ein endlicher metrischer Raum.

Um diejenigen Felder zu beschreiben, die von einem Turm auf v dominiert werden, sind die Begriffe Schale und Kugel hilfreich. Sei $e \in \mathbf{R}$ und $v \in K^2$. Dann heißt

$$S_e(v) := \{w \in K^2 \mid d(v,w) = e\}$$

die Schale und

$$B_e(v) := \{w \in K^2 \mid d(v,w) \leq e\}$$

die Kugel um v mit Radius e.

Damit dominiert ein Turm auf $v \in K$ genau die Felder in $B_1(v) = S_0(v) \cup S_1(v) = \{v\} \cup S_1(v)$.

Die Begriffe „Schale“ und „Kugel“ sind der euklidschen Metrik

$$d : \mathbf{R}^3 \to \mathbf{R}, (v, w) \mapsto \sqrt{(v_1 - w_1)^2 + (v_2 - w_2)^2 + (v_3 - w_3)^2}$$

des 3-dimensionalen Raumes entlehnt. Für die oben eingeführte Metrik sind beide Begriffe gewöhnungsbedürftig, der anschaulichere Begriff „Rook-Domain“ für $B_e(v)$ hat sich nicht durchgesetzt.

Stehen mehrere Türme auf einem Schachbrett, pro Feld jedoch höchstens einer, so empfiehlt sich die Verwendung einer Menge $C \subseteq K^2$ der mit Türmen besetzten Felder. Derjenige Bereich des Schachbretts, der von diesen Türmen dominiert wird, lässt sich durch $\bigcup_{v \in C} B_1(v)$ beschreiben. Damit ist Folgendes klar. Türme auf $C \subseteq K^2$ dominieren genau dann das gesamte Schachbrett, wenn $\bigcup_{v \in C} B_1(v) = K^2$.

Das klassische Überdeckungsproblem besteht hier nun in folgender Frage. Welches ist die kleinste Anzahl $K_8(2, 1)$ von Türmen auf einem gewöhnlichen, d.h. mit Kantenlänge 8 versehenen, 2-dimensionalen Schachbrett, die in der Lage sind,

jedes Feld in höchstens 1 Zug zu erreichen?

Die Antwort lautet $K_8(2, 1) = 8$, denn Türme auf $\{(0, 0), (0, 1), ..., (0, 7)\}$ erfüllen diese Eigenschaft und weniger als 8 Türmen gelingt dies offensichtlich nicht.

Man kann hier folgendermaßen sukzessive verallgemeinern.

(i) Man verwende statt 8 eine beliebige Kantenlänge $q \in \mathbf{N} = \{1, 2, ...\}$. Hier gilt $K_q(2, 1) = q$.

(ii) Man verwende ein n-dimensionales Schachbrett mit $n \in \mathbf{N}$. Leicht zu beweisen sind die Aussagen $K_q(1, 1) = 1$ und $K_q(2, 1) = q$. Mit mehr Aufwand kann man

$$K_q(3, 1) = \left\lceil \frac{q^2}{2} \right\rceil = \begin{cases} \frac{q^2}{2}, & \text{falls } q \text{ gerade,} \\ \frac{q^2+1}{2}, & \text{falls } q \text{ ungerade,} \end{cases}$$

zeigen. Zudem ist beispielsweise $K_2(4, 1) = 4$, $K_3(4, 1) = 9$, $K_4(4, 1) = 24$ bekannt, jedoch hat man bisher $K_5(4, 1)$ noch nicht bestimmen können.

(iii) Welches ist die kleinste Anzahl $K_q(n, e)$ von Türmen, die in der Lage sind,

jedes Feld in höchstens $e \in \mathbf{N}_0$ Zügen zu erreichen?

(iv) Man verwende andere Figuren, z.B. Könige, oder andere Bretter, z.B. wabenförmige mit sechseckigen Feldern.

Für das Packungsproblem betrachte man zwei Türme auf unterschiedlichen Feldern $v, w \in K^2$ eines gewöhnlichen Schachbretts. Offensichtlich lassen sich diejenigen Situationen, in denen kein Turm den anderen bedroht, d.h. innerhalb eines Zuges schlagen kann, durch die Bedingung $d(v, w) \geq 2$ charakterisieren. Auch $d(v, w) = 2$ wäre möglich, im Hinblick auf Verallgemeinerungsmöglichkeiten wird jedoch $\geq$ gewählt. Um auch mehr als zwei Türme betrachten zu können, wird die Minimaldistanz

$$d(C) := \min\{d(v, w) \mid v, w \in C \text{ und } v \neq w\}$$

für $C \subseteq K^2$ mit $|C| \geq 2$ eingeführt. Damit ist Folgendes klar. Türme auf $C \subseteq K^2$ mit $|C| \geq 2$ erfüllen genau dann die Eigenschaft, dass keiner den anderen innerhalb eines Zuges schlagen kann, wenn $d(C) \geq 2$.

Das klassische Packckungsproblem besteht hier nun in folgender Frage. Welches ist die größte Anzahl $A_8(2, 2)$ von Türmen auf einem gewöhnlichen Schachbrett (Kantenlänge 8, Dimension 2), die sich gegenseitig innerhalb von 1 Zug nicht schlagen können, d.h. für die $d(C) \geq 2$ gilt? Die Antwort lautet $A_8(2, 2) = 8$, denn Türme auf $C = \{(0, 0), (1, 1), ..., (7, 7)\}$ erfüllen die geforderte Eigenschaft und mehr als 8 Türme tun dies nicht.

Allgemeiner gilt $A_q(2, 2) = q$ und $A_q(n, 2) = q^{n-1}\, \forall n \in \mathbf{N} \setminus \{1\}$. Noch allgemeiner ist die Frage nach der größten Anzahl $A_q(n, d)$ von Türmen, die sich gegenseitig innerhalb von $d - 1$ Zügen nicht schlagen können, d.h. für die $d(C) \geq d$ gilt. Noch unbekannt sind bisher beispielsweise $A_3(6, 3)$ und $A_6(5, 3)$. Auch hier können andere Figuren und Bretter verwendet werden.

2 Grundlagen

Es werden nun einige (für sich betrachtet sehr trockene) Grundlagen bereitgestellt, die für den Aufbau der Theorie unablässig sind. Zur Veranschaulichung ist es oftmals hilfreich, sich an der vorangegangenen Motivation zu orientieren.

2.1 Vorbereitungen

Sei (R, d^R) ein endlicher metrischer Raum, d.h. sei R eine Menge mit $|R| \in \mathbf{N}$ und $d^R : R \times R \to \mathbf{R}$ eine Metrik. Im vorliegenden Beitrag werden metrische Eigenschaften von (R, d^R) und der durch $C \in \mathcal{P}(R)$ induzierten Unterräumen diskutiert. Dabei werden (in einem noch zu definierenden Sinne) extremale Mengen C gesucht. An vielen Stellen wird die Dreiecksungleichung nicht benötigt.

In einigen anderen Abhandlungen wird ein $\mathcal{M} \subseteq \mathcal{P}(R)$ vorgegeben und es werden nur die durch $C \in \mathcal{M}$ induzierten Unterräume betrachtet. Trägt R die algebraische Struktur einer Gruppe, eines Vektorraums o.ä., so kann $\mathcal{M}$ etwa aus den algebraischen Unterstrukturen bestehen. Derartige Ansätze führen in den (noch zu definierenden) Hamming-Räumen auf die Theorie der Gruppencodes und linearen Codes innerhalb der algebraischen Codierungstheorie.

Bei allen Untersuchungen wird der triviale Fall $|R| = 1$ üblicherweise stillschweigend ausgeschlossen. Die nächstgrößeren Fälle sind ebenfalls recht übersichtlich.

Ist $(R', d^{R'})$ ein weiterer endlicher metrischer Raum und ist $\varphi : R \to R'$ eine Bijektion mit $d^{R'}(\varphi(v), \varphi(w)) = d^R(v, w) \, \forall v, w \in R$, so heißen beide Räume *isometrisch* und φ eine *Isometrie*. Die Menge der Isometrien eines endlichen metrischen Raumes auf sich heißt *Autometriegruppe*.

Ist $a \in \mathbf{R}^+$, so ist auch $(R, a \cdot d^R)$ ein endlicher metrischer Raum.

Sei

$$D(C) := \{d^R(v, w) \mid v, w \in C\}$$

die Menge aller in einer Teilmenge $C \subseteq R$ auftretenden Abstände und $D^*(C) := D(C) \setminus \{0\}$. Weiter heißt

$$S_e(v) := \{w \in R \mid d^R(v, w) = e\}$$

die *Schale* und

$$B_e(v) := \{w \in R \mid d^R(v, w) \leq e\}$$

die *Kugel* um $v \in R$ mit Radius $e \in D(R)$. Zudem heißt

$$r(e) := \max\{e' \in D(R) \mid B_{e'}(v) \cap B_{e'}(w) = \emptyset \, \forall v, w \in R \text{ mit } d^R(v, w) \geq e\}$$

der *kritische Radius* bezüglich $e \in D^*(R)$. Er wächst monoton. Ist $C \subseteq R$, so heißt

$$p(C) := \max\{e' \in D(R) \mid B_{e'}(v) \cap B_{e'}(w) = \emptyset \, \forall v, w \in C \text{ mit } v \neq w\}$$

der *Packungsradius* von C. Zu $v, w \in R$ sei

$$V(v,w) := \{z \in R \mid d^R(v,z) + d^R(z,w) = d^R(v,w)\}$$

die *Verbindungsmenge* von v und w.

Sei $|C| \geq 1$. Setze $d(v,C) := \min\{d^R(v,w) \mid w \in C\}$ für $v \in R$. Dann heißt

$$t(C) := \max\{d(v,C) \mid v \in R\}$$

der *Überdeckungsradius* und $\Delta(C) := \max D(C)$ der *Durchmesser* von C. Es gilt $t(C) \leq e$ genau dann, wenn $\bigcup_{v \in C} B_e(v) = R$. Wird im Folgenden $t(C)$ oder $\Delta(C)$ verwendet, so sei stillschweigend $|C| \geq 1$ vorausgesetzt.

Durch die Bijektion

$$\psi : D(R) \setminus \{\Delta(R)\} \to D^*(R), e \mapsto \min\{e' \in D^*(R) \mid e' > e\}$$

wird der *Nachfolger* $\psi(e)$ von $e < \Delta(R)$ definiert. $\psi^{-1}(e)$ ist der *Vorgänger* von $e > 0$ in $D(R)$. Es gilt $\psi(r(e)) \leq e \leq 2\psi(r(e))$ und $\Delta(B_{r(e)}(v)) \leq \psi^{-1}(e) \, \forall v \in R$ und $e \in D^*(R)$.

Sei $|C| \geq 2$. Dann heißt $d(C) := \min D^*(C)$ die Minimaldistanz von C. Wird im Folgenden $d(C)$ verwendet, so sei stillschweigend $|C| \geq 2$ vorausgesetzt. Es gilt $r(d(C)) \leq p(C)$.

Der mit $e \in D(R)$ *assoziierte Graph* $G_e := (V,E)$ wird durch $V := R$ und $E := \{\{v,w\} \subseteq R \mid 0 < d^R(v,w) \leq e\}$ definiert. Der graphentheoretische Begriff der abgeschlossenen Nachbarschaft $N[v] := \{v\} \cup \{w \in V \mid v$ und w sind benachbart$\}$ stimmt dann mit dem der Kugel $B_e(v)$ überein.

Sei $G = (V,E)$ ein zusammenhängender endlicher Graph und $d_G(v,w)$ die kleinste Anzahl an Kanten eines Weges von v nach w. Setzt man $R := V$ und $d^R := d_G$, so ist (R, d^R) ein durch G induzierter endlicher metrischer Raum mit $D(R) = \{0, 1, ..., \Delta(R)\}$ und $r(e) = \lfloor \frac{e-1}{2} \rfloor$. Der mit 1 assoziierte Graph stimmt mit G überein.

Es ist hilfreich, folgende Charakterisierungen für endliche metrische Räume zu betrachten.

Definition 2.1 (i) (Distanzinvarianz) *Für alle $e \in D(R)$ ist $|B_e(v)|$ unabhängig von $v \in R$. Damit existieren alle $V_e := |B_e(v)|$. Hierzu gleichwertig ist die Forderung, dass für alle $e \in D(R)$ der Wert $|S_e(v)|$ unabhängig von $v \in R$ ist. $|S_e(v)|$ wird als* Valenz *bezeichnet.*

(ii) (Transitivität der Autometriegruppe) *Für alle* $v, v' \in R$ *existiert eine Autometrie* φ *mit* $\varphi(v) = v'$.

(iii) (Translationsinvarianz) $(R, \circ)$ *ist eine Quasigruppe und die Translationen* $\varphi_w : v \mapsto v \circ w$ *sowie* ${}_w\varphi : v \mapsto w \circ v$ *sind Autometrien.*

(iv) (Distanzregularität) *Für alle* $e, e', \bar{e} \in D(R)$ *ist* $|S_e(v) \cap S_{e'}(v')|$ *unabhängig von* $v, v' \in R$, *sofern* $d^R(v, v') = \bar{e}$.

(v) (Distanztransitivität der Autometriegruppe) *Für alle* $v, v', w, w' \in R$ *mit* $d^R(v, w) = d^R(v', w')$ *existiert eine Autometrie* φ *mit* $\varphi(v) = v'$ *und* $\varphi(w) = w'$.

(vi) (Existenz von Zwischenwerten) *Zu* $v, w \in R$ *und* $e \in D^*(R)$ *mit* $e < d^R(v, w)$ *existiert ein* $z \in V(v, w)$ *mit* $d^R(v, z) = e$.

(vii) (Graphischer Raum) (R, d^R) *wird durch einen Graphen induziert.*

Lemma 2.2 *Es gilt* (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) *und* (v) $\Rightarrow$ (iv) $\Rightarrow$ (i) *sowie* (v) $\Rightarrow$ (ii) *und* (vii) $\Rightarrow$ (vi).

Wie im Vorwort erwähnt, führt (iv) auf den Begriff des Association Scheme. Man kann leicht einen endlichen metrischen Raum mit sechs Elementen angeben, in dem (iii), jedoch nicht (iv) gilt. Auch wird (v) nicht durch (iv) impliziert, vgl. Brouwer/Cohen/Neumaier [11], (i) nicht durch (vii) und (vi) weder durch (iii) noch durch (v). Es gibt endliche metrische Räume, in denen (vi), jedoch nicht (vii) erfüllt ist, doch gilt folgender Zusammenhang.

Lemma 2.3 *Sei* (R, d^R) *ein endlicher metrischer Raum, in dem die Existenz von Zwischenwerten gewährleistet ist. Dann existiert ein* $a \in \mathbf{R}^+$, *so dass* $(R, a \cdot d^R)$ *ein graphischer Raum ist.*

Beweis: Sei $|R| \geq 2$. Setze $a := d(R)^{-1}$. Es gilt $|e - e'| \in D(R)\, \forall e, e' \in D(R)$ und damit $D(R) \subseteq a^{-1}\mathbf{N}_0$. Der mit a^{-1} assoziierte Graph induziert dann $(R, a \cdot d^R)$, da der kürzeste Wege von $v \in R$ nach $w \in R$ aus genau $a \cdot d^R(v, w)$ Kanten besteht. □

Zur Vorbereitung auf Späteres dienen folgende, sehr technische Hilfsaussagen.

Lemma 2.4 *Sei (R, d^R) ein endlicher metrischer Raum, in dem die Existenz von Zwischenwerten gewährleistet ist. Seien $v, w \in R$ und $d^R(v, w) \leq e \in D(R)$.*

(i) *Wenn $e > 0$, dann $B_{\psi(r(e))}(v) \cap B_{\psi(r(e))}(w) \neq \emptyset$.*

(ii) *Wenn $e < \Delta(R)$ und $\Delta(R) > 2r(\psi(e))$ sowie $\psi(e) \leq \min\{\bar{e} \in D(R) \mid \bar{e} > 2r(\psi(e))\}$, dann $B_{r(\psi(e))}(v) \cap B_{r(\psi(e))}(w) \neq \emptyset$.*

Beweis:

(i) Setze $e' := d^R(v, w) \leq e$. Im Fall $\psi(r(e')) \geq e'$ ist nichts zu zeigen. Sei $\psi(r(e')) < e'$. Dann $\exists v', w' \in R$ und $z' \in B_{\psi(r(e'))}(v) \cap B_{\psi(r(e'))}(w)$ mit $d^R(v, w) \geq e'$. Damit ist $d^R(v', z') < e'$. Also $\exists z \in V(v, w)$ mit $d^R(v, z) \leq \psi(r(e'))$. Somit gilt $d^R(w, z) = d^R(v, w) - d^R(v, z) \leq d^R(v', w') - d^R(v', z') \leq d^R(w', z') \leq \psi(r(e'))$. Hierdurch ist $z \in B_{\psi(r(e))}(v) \cap B_{\psi(r(e))}(w)$.

(ii) Im Fall $r(\psi(e)) \geq d^R(v, w)$ ist nichts zu zeigen. Sei $\psi(r(e')) < d^R(v, w)$. Dann $\exists z \in V(v, w)$ mit $d^R(v, z) = r(\psi(e))$. Wegen $d^R(v, w) < \min\{\bar{e} \in D(R) \mid \bar{e} > 2r(\psi(e))\}$ gilt zudem $d^R(w, z) = d^R(v, w) - r(\psi(e)) \leq r(\psi(e))$. Also ist $z \in B_{r(\psi(e))}(v) \cap B_{r(\psi(e))}(w)$. □

Nun lassen sich der kritische Radius, der Packungsradius und der Überdeckungsradius folgendermaßen zueinander in Beziehung setzen.

Satz 2.5 *Sei (R, d^R) ein endlicher metrischer Raum, in dem die Existenz von Zwischenwerten gewährleistet ist, und sei $C \subseteq R$ mit $|C| \geq 2$. Dann gilt*

$$r(d(C)) = p(C) \leq t(C).$$

Beweis: Lemma 2.4 (i) liefert $\psi(r(d(C))) > p(C)$. – Im Fall $t(C) = \Delta(R)$ ist nichts zu zeigen. Sei $t(C) < \Delta(R)$. Aufgrund der Existenz von Zwischenwerten ist $\bigcup_{v \in C} B_{\psi(t(C))}(v)$ nicht disjunkt, da bereits $\bigcup_{v \in C} B_{t(C)}(v) = R$ gilt. Also ist $\psi(t(C)) > p(C)$. □

Ist Existenz von Zwischenwerten nicht gewährleistet, so lassen sich leicht Situationen mit $r(d(C)) < p(C)$ oder $p(C) > t(C)$ konstruieren.

2.2 Extremale Mengen und Kardinalitäten

Es folgen nun die zentralen Begriffe dieses Beitrags.

Definition 2.6 *Sei $C \subseteq R$ und $e \in D(R)$.*

(i) *C heißt* e-unabhängig $:\Leftrightarrow v \notin \bigcup_{w \in C \setminus \{v\}} B_e(w) \, \forall v \in C \Leftrightarrow |C| \leq 1$ *oder* $d(C) > e$.

(ii) *C heißt* e-überdeckend *oder auch* e-dominant $:\Leftrightarrow \bigcup_{v \in C} B_e(v) = R \Leftrightarrow t(C) \leq e$.

(iii) *C heißt* e-irredundant $:\Leftrightarrow B_e(v) \setminus \bigcup_{w \in C \setminus \{v\}} B_e(w) \neq \emptyset \, \forall v \in C$.

Die Begriffe „Unabhängigkeit“, „Dominanz“ und „Irredundanz“ stammen aus der Graphentheorie. Jede e-unabhängige Menge ist auch e-irredundant.

Lemma 2.7 *Sei $e < \Delta(R)$. Dann folgt aus der e-Unabhängigkeit von C die Aussage*

$$B_{r(\psi(e))}(v) \cap B_{r(\psi(e))}(w) = \emptyset \, \forall v, w \in C \text{ mit } v \neq w.$$

Ist die Existenz von Zwischenwerten sowie $\Delta(R) > 2r(\psi(e))$ und

$$\psi(e) \leq \min\{\bar{e} \in D(R) \mid \bar{e} > 2r(\psi(e))\}$$

gewährleistet, so gilt auch die Umkehrung.

Beweis: Der Fall $|C| \leq 1$ ist trivial. – Sei $d(C) > e$. Dann gilt $r(d^R(v,w)) \geq r(\psi(e))$ und damit $B_{r(\psi(e))}(v) \cap B_{r(\psi(e))}(w) = \emptyset$. – Sei $d(C) \leq e$. Wähle $v, w \in C$ mit $v \neq w$ and $d^R(v,w) \leq e$. Dann gilt $B_{r(\psi(e))}(v) \cap B_{r(\psi(e))}(w) \neq \emptyset$ nach Lemma 2.4 (ii). □

Als Beispiel betrachte man einen durch einen graphischen Raum (R, d^R) und ein gerades $e \in D(R) \setminus \{\Delta(R)\}$. Dann gilt:

$$C \text{ ist } e\text{-unabhängig } \Leftrightarrow B_{\frac{e}{2}}(v) \cap B_{\frac{e}{2}}(w) = \emptyset \, \forall v, w \in C \text{ mit } v \neq w.$$

Eine e-unabhängige Menge C heißt (in $\mathcal{P}(R)$) *minimal* bzw. *maximal e-unabhängig*, falls es keine echte Teilmenge bzw. keine echte Obermenge von C in $\mathcal{P}(R)$ gibt, die ebenfalls e-unabhängig ist. Entsprechend sind *minimale* bzw. *maximale e-Dominanz* und *e-Irredundanz* definiert.

Jede Teilmenge einer e-unabhängigen Menge ist ebenfalls e-unabhängig, jede Obermenge einer e-überdeckenden Menge ist ebenfalls e-überdeckend, jede Teilmenge einer e-irredundanten Menge ist ebenfalls e-irredundant. Daher ist nur die leere Menge minimal e-unabhängig, nur R maximal e-überdeckend und nur die leere Menge minimal e-irredundant. Interessanter ist die Frage, welche Mengen im Fall $e \in D^*(R) \setminus \{\Delta(R)\}$ maximal e-unabhängig, minimal e-überdeckend oder maximal e-irredundant sind, während auch der Fall $e \in \{0, \Delta(R)\}$ trivial ist. Maximale e-Unabhängigkeit ist äquivalent zur Kombination aus e-Unabhängigkeit und e-Dominanz. Minimale e-Dominanz ist äquivalent zur Kombination aus e-Dominanz und e-Irredundanz.

Für jedes $e \in D(R)$ werden die folgenden sechs extremalen Kardinalitäten verwendet, deren Bezeichnungen in der Graphentheorie zum Standard geworden sind.

Definition 2.8 (i) *Die kleinste bzw. größte Kardinalität einer maximal e-unabhängigen Menge in $\mathcal{P}(R)$ wird mit $i(e)$ bzw. $\beta(e)$ bezeichnet.*

(ii) *Die kleinste bzw. größte Kardinalität einer minimal e-überdeckenden Menge in $\mathcal{P}(R)$ wird mit $\gamma(e)$ bzw. $\Gamma(e)$ bezeichnet.*

(iii) *Die kleinste bzw. größte Kardinalität einer maximal e-irredundanten Menge in $\mathcal{P}(R)$ wird mit $ir(e)$ bzw. $IR(e)$ bezeichnet.*

Der Zusatz „maximal" bzw. „minimal" kann in den Definitionen von $\beta(e)$, $\gamma(e)$ und $IR(e)$ entfallen. Werden die Begriffe e-Unabhängigkeit bzw. e-Dominanz mittels $d(C) = \psi(e)$ anstelle von $d(C) \geq \psi(e)$ bzw. mittels $t(C) = e$ anstelle von $t(C) \leq e$ definiert, so ist zu prüfen, ob der Wert der obigen extremalen Kardinalitäten dadurch verändert wird.

Es gilt die leicht einsehbare Aussage

$$1 \leq ir(e) \leq \gamma(e) \leq i(e) \leq \beta(e) \leq \Gamma(e) \leq IR(e) \leq |R|,$$

vgl. Cockayne/Hedetniemi/Miller [16]. Hinreichend für $\gamma(e) = i(e)$ ist die Forderung, dass G_e keinen bipartiten Graphen auf $1+3$ Ecken als induzierten Untergraphen enthält. Diese und ähnliche Aussagen werden beispielsweise in Jacobson/Peters [30] diskutiert. Vgl. auch Hedetniemi/Lasker [28] und deren Referenzen.

Über die Kardinalitäten $ir(e)$, $\Gamma(e)$ und $IR(e)$ ist (zumindest in den noch zu definierenden Sequenzräumen) nur sehr wenig bekannt, $i(e)$ wurde erst vor kurzem etwas intensiver untersucht. Daher befasst sich dieser Beitrag hauptsächlich mit $\gamma(e)$ und $\beta(e)$.

3 Der Sequenzraum

Sei K eine Menge mit $q := |K| \in \mathbf{N}$. Ist $n \in \mathbf{N}$, so heißt (K^n, d^{K^n}) *Sequenzraum* über dem *Alphabet* K und $C \subseteq K^n$ wird als *q-närer (Block-)Code der Länge* n bezeichnet. Der triviale Fall $q = 1$ wird üblicherweise stillschweigend ausgeschlossen. Wegen $R = R^1$ kann jeder endliche metrische Raum als Sequenzraum aufgefasst werden.

Beim *gemischten Sequenzraum* $R = \times_{x=1}^{n} K_x$ verwendet man Alphabete unterschiedlicher Kardinalität $q_x \geq 2$, d.h. es gibt $x, x' \in \{1, 2, ..., n\}$ mit $q_x \neq q_{x'}$. Die Teilmengen von R heißen hier gemischte Codes.

Die *Hamming-Metrik* d_H mit

$$d_H(v, w) := |\{x \in \{1, 2, ..., n\} \mid v_x \neq w_x\}|$$

für $v = (v_1, v_2, ..., v_n), w = (w_1, w_2, ..., w_n) \in K^n$ ist die gebräuchlichste Metrik des Sequenzraumes. (K^n, d_H) heißt der *Hamming-Raum*.

Satz 3.1 *Der Hamming-Raum (K^n, d_H) ist graphisch und translationsinvariant, seine Autometriegruppe ist distanztransitiv. Es gilt $D(K^n) = \{0, 1, ..., n\}$ und $r(e) = \lfloor \frac{e-1}{2} \rfloor$ sowie*

$$V_e = \sum_{k=0}^{e} \binom{n}{k} (q-1)^k.$$

Beweis: Offensichtlich gilt $\Delta(K^n) = n$. Ist $d_G(v, w)$ die kleinste Anzahl an Kanten eines Weges von v nach w im mit 1 assoziierten Graphen, so folgt $(K^n, d_H) = (K^n, d_G)$ und damit $D(K^n) = \{0, 1, ..., n\}$ und $r(e) = \lfloor \frac{e-1}{2} \rfloor$. Weiter ist $V_e = \sum_{k=0}^{e} |S_k(v)| = \sum_{k=0}^{e} \binom{n}{k} (q-1)^k$. Wird K mit einer beliebiegen Quasigruppenstruktur versehen, so zeigt sich die Translationsinvarianz. Zum Nachweis der Distanztransitivität sei $d_H(v, w) = d_H(v', w')$. Setze $I(v, w) := \{x \in \{1, 2, ..., n\} \mid v_x \neq w_x\}$. Dann $\exists \alpha \in \mathbf{S}_n$ mit $\alpha(I(v, w)) = I(v', w')$. Setze $\bar{\alpha} : (z_1, z_2, ..., z_n) \mapsto (z_{\alpha(1)}, z_{\alpha(2)}, ..., z_{\alpha(n)})$. Zu jedem $x \in \{1, 2, ..., n\} \, \exists \pi_x \in \mathbf{S}_K$ mit $\pi_x(\bar{\alpha}(v)_x) = v'_x$ und $\pi_x(\bar{\alpha}(w)_x) = w'_x$. Setze $\tilde{\pi} : (z_1, z_2, ..., z_n) \mapsto (\pi_1(z_1), \pi_2(z_2), ..., \pi_n(z_n))$. Damit ist $\tilde{\pi} \circ \bar{\alpha}$ die gesuchte Autometrie. $\square$

Im Hamming-Raum sind die Kardinalitäten $A_q(n,d) := \beta(d-1)$ und $K_q(n,e) := \gamma(e)$ intensiv untersucht worden und bilden den Schwerpunkt der kombinatorischen Codierungstheorie, vgl. etwa MacWilliams/Sloane [42], Vaessens/Aarts/van Lint [59], Bogdanova et al. [7], [8], Quistorff [47] sowie Cohen et al. [17] und deren Referenzen. Zudem wurde kürzlich auch $K_q(n,e,e+1) := i(e)$ und die Verallgemeinerung $K_q(n,e,d)$ untersucht, vgl. Quistorff [48], Blokhuis et al. [5], Östergård/Quistorff/Wassermann [44].

Der *gemischte Hamming-Raum* $(R = \times_{x=1}^{n} K_x, d_H)$ ist ebenfalls graphisch, jedoch nicht distanzregulär. (Es lässen sich für $e = e' = \bar{e} = 1$ leicht Schnittmengen von Schalen unterschiedlicher Kardinalität angeben.) Wird jedes Alphabet mit einer Quasigruppenstruktur versehen, so zeigt sich die Translationsinvarianz. Im Fall $R = \{0,1,2\}^{n_3} \times \{0,1\}^{n_2}$ ist $K_{3,2}(n_3,n_2,e) := \gamma(e)$ untersucht worden, vgl. Cohen et al. [17] und deren Referenzen.

Eine andere, häufig verwendete Metrik des Sequenzraumes ist die *Lee-Metrik* d_L mit

$$d_L(v,w) := \sum_{x=1}^{n} d_L(v_x,w_x)$$

und

$$d_L(v_x,w_x) := \min\{|v_x - w_x|, q - |v_x - w_x|\}$$

für $v,w \in K^n$, wobei als Alphabet die zyklische Gruppe $K = \mathbf{Z}/q\mathbf{Z}$ zu verwenden und für obiges Minimum diese mit der Menge ihrer Repräsentanten $\{0,1,...,q-1\} \subseteq \mathbf{Z}$ zu identifizieren ist. (K^n, d_L) heißt der *Lee-Raum.*

Im Sequenzraum mit $q \in \{2,3\}$ können Hamming- und Lee-Metrik miteinander identifiziert werden. Zudem sind $(\{0,1,2,3\}^n, d_L)$ und $(\{0,1\}^{2n}, d_H)$ isometrisch. (Um dies einzusehen, verwende man die Abbildung $\varphi : 0 \mapsto (0,0), 1 \mapsto (1,0), 2 \mapsto (1,1), 3 \mapsto (0,1)$).

Satz 3.2 *Der Lee-Raum ist graphisch und translationsinvariant. Im Fall $n = 1$ oder $q \leq 4$ ist seine Autometriegruppe distanztransitiv, andernfalls ist die Distanzregularität verletzt. Es gilt $D(K^n) = \{0,1,...,n\lfloor \frac{q}{2} \rfloor\}$ und $r(e) = \lfloor \frac{e-1}{2} \rfloor$. Für $e \in D(K^n)$ mit $e < \frac{q}{2}$ gilt*

$$V_e = \sum_{k=0}^{\min\{n,e\}} 2^k \binom{n}{k} \binom{e}{k}.$$

Beweis: Offensichtlich gilt $\Delta(K^n) = n\lfloor\frac{q}{2}\rfloor$. Für die Translationsinvarianz verwende man die Addition in K. Die Distanztransitivität ist im Fall $n = 1$ trivial und folgt im Fall $q \leq 4$ aus Satz 3.1. Für die verletzte Distanzregularität im Fall $n \geq 2$ und $q \geq 5$ wähle $e = e' = 1$ und $\bar{e} = 2$ sowie $v = (0, 0, ..., 0)$, $v' = (1, 1, 0, 0, ..., 0)$, $v = (2, 0, 0, ..., 0)$. Die Berechnung von V_e ist aufwendig und findet sich in Astola [4]. Alle anderen Nachweise verlaufen analog zu Satz 3.1. □

Es gibt für den Lee-Raum Untersuchungen zur Kardinalität $A_q^L(n, d) := \beta(d - 1)$. Der gemischte Lee-Raum scheint hingegen bisher kaum betrachtet worden zu sein.

Bei der sogenannten Codierung mit Permutationen verwendet man die symmetrische Gruppe $\mathbf{S}_n$, die mit $\{v \in \{1, 2, ..., n\}^n \mid v_x \neq v_{x'}$ für $x \neq x'\}$ identifiziert wird. Es liegt also ein Unterraum des Sequenzraumes vor. $(\mathbf{S}_n, d_H)$ heißt der *Hamming-Permutationsraum.*

Satz 3.3 *Der Hamming-Permutationsraum ist translationsinvariant und, abgesehen vom pathologischen Fall $n = 1$, nicht graphisch. Die Existenz von Zwischenwerten ist genau dann gewährleistet, wenn $n \leq 2$. Im Fall $n \leq 3$ ist die Autometriegruppe distanztransitiv, andernfalls ist die Distanzregulatrität verletzt. Es gilt $D(\mathbf{S}_n) = \{0, 2, 3, ..., n\}$ und*

$$r(e) = \begin{cases} 0, & \textit{falls } e \in D^*(\mathbf{S}_n) \cap \{3, 4\}, \\ \lfloor\frac{e-1}{2}\rfloor, & \textit{falls } e \in D^*(\mathbf{S}_n) \setminus \{3, 4\}, \end{cases}$$

sowie

$$V_e = \sum_{k=0}^{e} \binom{n}{k} k! \sum_{x=0}^{k} \frac{(-1)^x}{x!}.$$

Beweis: Offensichtlich gilt $D(\mathbf{S}_n) = \{0, 2, 3, ..., n\}$. Sei $e \in D^*(\mathbf{S}_n)$. Im Fall $e \leq 4$ folgt $r(e) = 0$. Andernfalls gilt $r(e) \leq \lfloor\frac{e-1}{2}\rfloor$ und $\frac{e}{2} \leq \psi(r(e))$, d.h. $\lfloor\frac{e-1}{2}\rfloor \leq r(e)$. Die Hintereinanderausführung von Permutationen induziert Translationsinvarianz. Wegen $1 \notin D(\mathbf{S}_n)$ ist der Raum nicht graphisch. Zum Nachweis der verletzten Existenz von Zwischenwerten im Fall $n \geq 3$ wählt man $v, w \in \mathbf{S}_n$ mit $d_H(v, w) = 3$ und $e = 2$. Für die Distanztransitivität im Fall $n = 3$ beachte man, dass nicht nur jedes $\pi \in \mathbf{S}_3$ (mittels $\alpha \mapsto \alpha \circ \pi$) sondern auch jede Permutation von $\{(1, 2, 3), (2, 3, 1), (3, 1, 2)\}$ und jede Permutation von $\{(1, 3, 2), (2, 1, 3), (3, 2, 1)\}$ eine Autometrie induziert. Im Fall $n \geq 4$ wählt man zum Nachweis der verletzten Distanzregularität $e =$

$e' = 2$ und $\bar{e} = 4$. Die Anzahl der fixpunktfreien Permutationen in $\mathbf{S}_k$ beträgt bekanntlich $k! \sum_{x=0}^{k} \frac{(-1)^x}{x!} =: F_k(k)$. (Eine Verallgemeinerung wird in Satz 5.6 verwendet.) Hieraus folgt $V_e = \sum_{k=0}^{e} |S_e((1,2,...,n))| = \sum_{k=0}^{e} \binom{n}{k} F_k(k)$. $\square$

Es gibt erste Untersuchungen der Kardinalitäten $\beta(e)$, $\gamma(e)$ und $i(e)$ im Hamming-Permutationsraum, vgl. Quistorff [47], [49], Tarnanen [58] und deren Referenzen. Setze $A_n(d) := \beta(\psi^{-1}(d))$ für $d \in D^*(\mathbf{S}_n)$.

Auch $J_{k,n} := \{v \in \{0,1\}^n \mid \sum_{x=1}^{n} v_x = k\}$ mit $k \in \{1,2,...,n-1\}$ ist ein (beliebter) Unterraum des Sequenzraumes. Setzt man $d_J(v,w) := \frac{1}{2} d_H(v,w)$ für alle $v,w \in J_{k,n}$, so heißt $(J_{k,n}, d_J)$ der *Johnson-Raum*. Er ist graphisch, es gilt $D(J_{k,n}) = \{0,1,...,\min\{k,n-k\}\}$ und $r(e) = \lfloor \frac{e-1}{2} \rfloor$. Seine Autometriegruppe ist distanztransitiv. (Hierzu beachte man, dass jede Permutation aus $\mathbf{S}_n$ eine Autometrie induziert.) Da die Räume $(J_{k,n}, d_J)$ und $(J_{n-k,n}, d_J)$ isometrisch sind, genügt es, den Fall $2k \leq n$ zu diskutieren. Sei X eine Menge mit $|X| = n \in \mathbf{N}$ und $k \in \mathbf{N}$ mit $2k \leq n$. Setzt man $R := \{A \in \mathcal{P}(X) \mid k = |A|\}$ und $d^R(A,B) := |A \setminus B|$, so ist auch (R, d^R) isometrisch zu $(J_{k,n}, d_J)$. Eine Menge $C \subseteq J_{k,n}$ ist in $(J_{k,n}, d_J)$ genau dann $(e-1)$-unabhängig, wenn $d_H(v,w) \geq 2e \,\forall v,w \in C$ mit $v \neq w$. Aufgrund dieser Verbindung zur Hamming-Metrik setze man im Johnson-Raum $A(n,2e,k) := \beta(e-1)$.

Sowohl im Sequenzraum als auch in den erwähnten Unterräumen sind weitere Metriken untersucht worden, vgl. etwa Davydov [19], Deza/Huang [22] und deren Referenzen.

Enomoto/Katona [24] und Brightwell/Katona [10] diskutieren folgende Modifikation des Johnson-Raums. Sei X eine Menge mit $|X| = n \in \mathbf{N}$ und sei $k \in \mathbf{N}$ mit $2k \leq n$. Setze $R := \{\{A_1, A_2\} \subseteq \mathcal{P}(X) \mid k = |A_1| = |A_2|$ und $A_1 \cap A_2 = \emptyset\}$ und $d^R(\{A_1,A_2\},\{B_1,B_2\}) := \min\{|A_1 \setminus B_1| + |A_2 \setminus B_2|, |A_1 \setminus B_2| + |A_2 \setminus B_1|\}$.

4 Anwendungen

4.1 Schachbrettprobleme

Ist (R, d^R) ein graphischer Raum, so kann man R als Menge der Felder eines verallgemeinerten Schachbretts und $S_1(v)$ als Menge der möglichen Züge einer auf $v \in R$ stehenden Figur deuten. Sind andersherum eine Menge R und eine Figur F mit ihren möglichen Zügen $(S_1(v))_{v \in R}$ gegeben, so erhält man hieraus einen Graphen und einen endlichen metrischen Raum (R, d_F), sofern $w \in S_1(v) \Rightarrow v \in S_1(w)$ gilt, d.h. die Züge umkehrbar sind, und sofern von jedem Feld aus jedes andere Feld in endlich vielen Zügen erreicht werden kann. Ist diese Erreichbarkeit wie beim Läufer auf dem gewöhnlichen Schachbrett K^2 nicht gegeben, so kann man durch eine geeignete Partitionierung von R mehrere endliche metrische Räume gewinnen.

Ist $R = K^n$ und F ein Turm, so gilt $d_F = d_H$, vgl. auch Golomb/Posner [27]. Damit ist $\beta(1)$ die maximale Anzahl sich nicht gegenseitig bedrohender Türme, $\gamma(1)$ die minimale Anzahl von Türmen, die K^n gemeinsam dominieren und $i(1)$ die minimale Anzahl von Türmen, auf die beide Eigenschaften zutreffen.

Auch andere Figuren, neue und klassische Schachfiguren, sind für K^n, insbesondere im Fall $n = 2$, und für andere Schachbretter betrachtet worden, vgl. etwa Fricke et al. [26], Bode/Harborth [6], Allison/Yee/McGaughey [3].

Sei $R = (\mathbf{Z}/q\mathbf{Z})^n$ ein sogenanntes toroidales Schachbrett und sei F eine Figur, die von jedem Feld in endlich vielen Zügen jedes andere Feld erreichen kann. Existiert eine Menge $Z_F \subseteq R \setminus \{(0, 0, ..., 0)\}$ mit $S_1(v) = v + Z_F \, \forall v \in R$, so ist (R, d_F) ein translationsinvarianter Raum. Setzt man beispielsweise $Z_F := J_{1,n} \cup -J_{1,n} \subseteq R \setminus \{(0, 0, ..., 0)\}$, so erhält man eine Figur, die an eine Mischung aus Bauer und König auf einem toroidalen Schachbrett erinnert, und (R, d_F) ist der Lee-Raum. Für den Fall, dass F eine Dame ist, vgl. Pólya [45], Burger/Mynhardt/Cockayne [14].

4.2 Fehlerkorrigierende Codes

Man betrachte die Kommunikation eines Senders mit einem Empfänger über einen fehleranfälligen Übertragungskanal unter Verwendung eines endlichen metrischen Raumes (R, d^R) und einer Menge $C \subseteq R$. Häufig wird dabei ein Hamming- oder Lee-Raum verwendet. Generell werden Elemente aus C gesendet und Elemente aus R empfangen. Wird $v \in C$ gesendet und $w \in R$ empfangen, so gibt $d^R(v, w)$ die Schwere des aufgetretenen Fehlers an.

Der Empfänger steht vor der Aufgabe, aus w ein $v' \in C$ zu konstruieren, das mit hoher Wahrscheinlichkeit mit v übereinstimmt. Hierzu wird zunächst das eindeutige $\bar{e} \in D(R)$ mit $A := S_{\bar{e}}(w) \cap C \neq \emptyset$ und $S_{e'}(w) \cap C = \emptyset \, \forall e' \in D(R)$ mit $e' < \bar{e}$ bestimmt. Falls $|A| \geq 2$, so wird v' willkürlich aus A gewählt, andernfalls liegt $v' \in A$ eindeutig fest. Bei dieser sogenannten *Maximum-Likelihood-Decodierung* stellt sich die Frage, welche Eigenschaften C besitzten muss, um bei gegebenem $e \in D(R)$ jeden Fehler der Schwere höchstens e mit völliger Sicherheit korrigieren zu können, d.h. um $A = \{v\}$ sicherzustellen.

Zu diesem Zweck wird folgender Begriff eingeführt. Sei $e \in D(R)$ und $C \subseteq R$. Genau dann heißt C eine *e-fehlerkorrigierende* Menge, wenn $e \leq p(C)$, d.h. wenn $B_e(v) \cap B_e(w) = \emptyset \, \forall v, w \in C$ mit $v \neq w$. Um zusätzlich die durch die Wahl von $C \subseteq R$ verursachte Redundanz der oben beschriebenen Kommunikation zu minimieren, ist die größte Kardinalität $f(e)$ einer e-fehlerkorrigierenden Menge in $\mathcal{P}(R)$ gesucht.

Trivialerweise gilt $1 = f(\Delta(R)) \leq f(e) \leq f(0) = |R|$. Zur Charakterisierung der e-fehlerkorrigierenden Mengen mit $e \in D^*(R)$ setze $\vartheta(e) := \max\{e' \in D^*(R) \mid e > r(e')\}$.

Satz 4.1 *Jede $\vartheta(e)$-unabhängige Menge ist e-fehlerkorrigierend und es gilt $f(e) \geq \beta(\vartheta(e))$. Ist die Existenz von Zwischenwerten gewährleistet, so ist auch jede e-fehlerkorrigierende Menge $\vartheta(e)$-unabhängig und es gilt $f(e) = \beta(\vartheta(e))$. Ist der Raum graphisch, so gilt zudem $\vartheta(e) = \min\{2e, \Delta(R)\}$.*

Beweis: C ist genau dann $\vartheta(e)$-unabhängig, wenn $|C| \leq 1$ oder $e \leq r(d(C))$. Hieraus folgt $e \leq p(C)$. Ist die Existenz von Zwischenwerten gewährleistet, so gilt nach Satz 2.5 auch die Umkehrung. Ist der Raum graphisch, so gilt

$$\vartheta(e) = \max\left\{e' \in D^*(R) \,\middle|\, e > \left\lfloor \frac{e'-1}{2} \right\rfloor \right\} = \begin{cases} 2e, & \text{falls } 2e < \Delta(R), \\ \Delta(R), & \text{andernfalls.} \end{cases}$$

□

Im Hamming-Permutationsraum mit $n \geq 4$ gilt $\vartheta(2) = 4$ und trotzdem existiert eine 3-unabhängige, 2-fehlerkorrigierende Menge.

Der Begriff der e-fehlererkennenden Menge wird in der Literatur in Abhängigkeit von der gewählten Decodierung unterschiedlich definiert. Manchmal stimmt er mit der e-Unabhängigkeit überein, vgl. etwa Willems [61], manchmal wird $B_e(v) \cap B_{e'}(w) = \emptyset \, \forall v, w \in C$ mit $v \neq w$ für ein geeignetes e', etwa $e' = r(d(C))$ gefordert, vgl. Heise/Quattrocchi [29], Quistorff [47].

4.3 Garantiesysteme

Sei R eine Menge endlich vieler möglicher Ergebnisse eines Zufallsexperiments, auf das Vorhersagen abgegeben, d.h. Wetten abgeschlossen werden können. Für ein Ergebnis $v \in R$ messe $d^R(v, w)$ den Fehler einer Vorhersage

$w \in R$. Zu $e \in D(R)$ heißt $C \subseteq R$ ein e-*Garantiesystem* genau dann, wenn für jedes Ergebnis $v \in R$ (mindestens) eine Vorhersage $w \in C$ mit $d^R(v,w) \le e$ existiert. Damit sind die Begriffe e-Garantiesystem und e-überdeckende Menge äquivalent. Gesucht ist die kleinste Kardinalität eines e-Garantiesystems.

Beim Fußballtoto besteht das Zufallsexperiment aus n Fußballspielen mit je 3 möglichen Ausgängen (Sieg oder Unentschieden oder Niederlage der Heimmannschaft). Zur Modellierung wird $R := \{0,1,2\}^n$, versehen mit der Hamming-Metrik d_H, verwendet und $d_H(v,w)$ bestimmt für ein Ergebnis v die Gewinnklasse einer Vorhersage w. Häufig erscheint nicht in jedem Fußballspiel jeder der 3 Ausgänge realistisch. Für eine Modifikation zerlege man daher n in $n_3 + n_2 + n_1$, sofern in genau n_k Spielen nur je k Ausgänge in Erwägung gezogen werden sollen, und betrachte den durch $R' := \{0,1,2\}^{n_3} \times \{0,1\}^{n_2} \times \{0\}^{n_1}$ induzierten Unterraum. Bei der Suche nach e-Garantiesystemen (minimaler Kardinalität) dieses Unterraums kann o.B.d.A. $n_1 = 0$ gewählt werden. Ist $\min\{n_3, n_2\} > 0$, so liegt ein gemischter Hamming-Raum vor. Für weitere Modifikationen vgl. Cohen et al. [17] und deren Referenzen. Darüber hinaus sind im Fußballtoto auch Deutungen von $\beta(e)$ und $i(e)$ denkbar.

Zur Modellierung von Lotterien vom Typ „k aus n“, wie z.B. „6 aus 49“, verwende man den zum Johnson-Raum isometrischen (R, d^R) mit $R = \{A \in \mathcal{P}(X) \mid k = |A|\}$ für $|X| = n$ und $d^R(A,B) = |A \setminus B|$. In Analogie zum Toto bestimmt $d^R(A,B)$ die Gewinnklasse und gesucht sind e-Garantiesysteme (minimaler Kardinalität). Man verwendet $L(n,k,k,k-e) := \gamma(e)$. Für eine Modifikation des Problems wird nur eine Teilmenge $X' \subseteq X$ in Erwägung gezogen. Gesucht ist ein System $C \subseteq R' := \{A \in \mathcal{P}(X') \mid k = |A|\}$ derart, dass für jedes $B \in R$ mit $|B \cap X'| = p$ (mindestens) ein $A \in C$ mit $d^R(A,B) \le e$ existiert. Die minimale Kardinalität eines solchen Systems wird mit $L(|X'|, k, p, k-e)$ bezeichnet. Vgl. Colbourn [18], Li/van Rees [36], Li [35] und deren Referenzen. Oder aber [43].

4.4 Quasigruppen

Sei K eine endliche Menge und $n \in \mathbf{N}$. Man verwende

$$v^{(x)}\#y := (v_1, v_2, ..., v_{x-1}, y, v_{x+1}, v_{x+2}, ..., v_n) \in K^n$$

für $v^{(x)} = (v_1, v_2, ..., v_{x-1}, v_{x+1}, v_{x+2}, ..., v_n) \in K^{n-1}$ und $y \in K$. Sei $A : D \to K$ eine Abbildung mit Definitionsbereich $D \subseteq K^n$. Genau dann heißt

(K, D, A) eine *partielle n-Quasigruppe der Größe $|D|$*, wenn

$$A(v^{(x)}\#y) = A(v^{(x)}\#y') \Rightarrow y = y' \,\forall v^{(x)}\#y, v^{(x)}\#y' \in D.$$

Zudem heißt eine partielle n-Quasigruppe (K, D, A) genau dann *voll*, wenn der Definitionsbereich D von A maximal ist, d.h. jede Erweiterung die algebraische Struktur zerstört.

Jede partielle n-Quasigruppe (K, D, A) induziert einen 1-unabhängigen Code $C = \{(v, A(v)) \in K^{n+1} \mid v \in D\}$ der Kardinalität $|D|$ im Hamming-Raum (K^{n+1}, d_H) und umgekehrt. C ist genau dann maximal 1-unabhängig, wenn (K, D, A) voll ist. Damit ist $i(1)$ die geringste Größe einer vollen partiellen n-Quasigruppe, vgl. Quistorff [46] und seine Referenzen.

5 Abschätzungen

Die Bestimmung der extremalen Kardinalitäten $\beta(e)$, $\gamma(e)$, $i(e)$ usw. ist in vielen endlichen metrischen Räumen sehr schwierig und nur in wenigen Spezialfällen bisher gelungen. Daher sind bei gegebenem $e \in D(R)$ eine möglichst große untere Schranke α' und eine möglichst kleine obere Schranke α'' für die betrachtete Kardinalität gesucht. Im Idealfall $\alpha' = \alpha''$ ist das Problem natürlich gelöst. Sind $\alpha', \alpha'' \in \mathbf{R}^+$, so können sie durch $\lceil \alpha' \rceil, \lfloor \alpha'' \rfloor \in \mathbf{N}$ ersetzt werden. Im Folgenden wird auf diese Rundungen nicht mehr explizit hingewiesen.

Jede Konstruktion einer e-unabhängigen Menge C rechtfertigt die untere Schranke $\beta(e) \geq |C|$. Ist C sogar maximal e-unabhängig, so impliziert dies zudem die obere Schranke $i(e) \leq |C|$. Entsprechendes gilt für die Konstruktion (minimal) e-überdeckender und (maximal) e-irredundanter Mengen. Man spricht hier von konstruktiven Schranken.

Ein Nichtexistenznachweis einer e-unabhängigen Menge der Kardinalität $\alpha'' + 1 \in \mathbf{N}$ impliziert die obere Schranke $\beta(e) \leq \alpha''$. Entsprechendes gilt auch für $\gamma(e)$ und $IR(e)$. Man spricht hier von destruktiven Schranken. Ein Nichtexistenznachweis einer maximal e-unabhängigen Menge der Kardinalität $\alpha' - 1 \in \mathbf{N}$ impliziert jedoch nicht notwendigerweise $i(e) \geq \alpha'$, vgl. Östergård/Quistorff/Wassermann [44].

Seien (R, d^R), $(R', d^{R'})$ und $(\bar{R}, d^{\bar{R}})$ endliche metrische Räume, seien $e \in D(R)$, $e' \in D(R')$ und $\bar{e} \in D(\bar{R})$. Zur besseren Unterscheidung sei die größte Kardinalität einer e-, e'-, bzw. $\bar{e}$-unabhängigen Menge in diesen Räumen mit

$\beta(e)$, $\beta'(e')$ bzw. $\bar{\beta}(\bar{e})$ bezeichnet. Ebenso wird mit den anderen Mengen und Funktionen verfahren. Lässt sich aus jeder e-unabhängigen Menge $C \subseteq R$ eine $\bar{e}$-unabhängige Menge $\bar{C} \subseteq \bar{R}$ mit $|\bar{C}| = |C|$ konstruieren, so folgt $\beta(e) \leq \bar{\beta}(\bar{e})$. Werden zur Konstruktion von $\bar{C}$ eine e-unabhängige Menge $C \subseteq R$ und eine e'-unabhängige Menge $C' \subseteq R'$ verwendet und gilt $|\bar{C}| = g(|C|, |C'|)$, so folgt $g(\beta(e), \beta'(e')) \leq \bar{\beta}(\bar{e})$. Entsprechendes gilt für die anderen extremalen Kardinalitäten. Die dabei gewonnenen Abschätzungen werden als induzierte Schranken bezeichnet. Sie können sowohl konstruktiv als auch destruktiv genutzt werden.

5.1 Induzierte Schranken

Zunächst werden Situationen betrachtet, in denen höchstens zwei endliche metrische Räume auftreten. Stimmen diese beiden Räume überein, so sieht man sofort, dass die Funktionen β und γ monoton fallen. Sind d^R und $\bar{d}^R$ hingegen zwei Metriken auf übereinstimmenden Mengen $R = \bar{R}$ und existiert ein $a \in \mathbf{R}^+$ mit $d^R(v,w) \leq a\bar{d}^R(v,w)\,\forall v,w \in R$, so folgt $\beta(e) \leq \bar{\beta}(\bar{e})$ und $\gamma(e) \leq \bar{\gamma}(\bar{e})$ mit $\bar{e} := \max\{\tilde{e} \in D(\bar{R}) | a\tilde{e} \leq e\}$. Als Beispiel für $a = 1$ betrachte man zwei Figuren F und $\bar{F}$ auf einem Schachbrett $R = \bar{R}$ mit $S_1(v) \supseteq \bar{S}_1(v)$, etwa Dame und König. Im Fall von Hamming- und Lee-Metrik auf $(\mathbf{Z}/q\mathbf{Z})^n$ erhält man

$$A_q(n,d) \leq A_q^L(n,d) \leq A_q\left(n, \left\lceil \frac{d}{a} \right\rceil\right) \text{ mit } a := \left\lfloor \frac{q}{2} \right\rfloor.$$

Hilfreich für unabhängige Mengen ist folgende Aussage, bei der häufig nur der Spezialfall $|J| = 1$ benötigt wird.

Lemma 5.1 *Sei $R = \biguplus_{j \in J} R_j$ eine Dekomposition und $\varphi : R \to \bar{R}$ eine Abbildung. Setze*

$$M := \{(d^R(v,w), d^{\bar{R}}(\varphi(v), \varphi(w))) \in D(R) \times D(\bar{R}) \mid j \in J \text{ und } v, w \in R_j\}.$$

Zu $e \in D(R)$ setze $M_e := \{\bar{e} \in D(\bar{R}) \mid (e, \bar{e}) \in M\}$, im Fall $\bigcup_{\tilde{e} > e} M_{\tilde{e}} \neq \emptyset$ setze zudem $\omega(e) := \min \bigcup_{\tilde{e} > e} M_{\tilde{e}} \in D(\bar{R})$. Dann gilt

$$\frac{\beta(e)}{|J|} \leq \bar{\beta}(\bar{\psi}^{-1}(\omega(e)))$$

für alle $e \in D(R) \setminus \{\Delta(R)\}$ mit $\omega(e) > 0$.

Beweis: Sei $C \subseteq R$ eine e-unabhängige Menge mit $|C| = \beta(e)$. Es existiert ein $j \in J$ mit $|C \cap R_j| \geq \frac{|C|}{|J|}$. Für $v, w \in C \cap R_j$ mit $v \neq w$ gilt $d^{\bar{R}}(\varphi(v), \varphi(w)) \geq \omega(e) > 0$. Setze $\bar{e} := \bar{\psi}^{-1}(\omega(e))$, dann ist $\varphi(C \cap R_j)$ eine $\bar{e}$-unabhängige Menge mit

$$\frac{\beta(e)}{|J|} = \frac{|C|}{|J|} \leq |C \cap R_j| = |\varphi(C \cap R_j)| \leq \bar{\beta}(\bar{e}).$$

□

Es folgen einige Anwendungen dieses Lemmas, die zum Teil mit wenig Mühe verbessert werden können. In Hamming-Räumen gilt:

(i) (Verlängerung)
$$A_q(n, d) \leq A_q(n + 1, d),$$

(ii) (Punktierung)
$$A_q(n, d) \leq A_q(n - 1, d - 1) \text{ für } d \geq 2,$$

(iii) (Ableitung)
$$\frac{A_q(n, d)}{q} \leq A_q(n - 1, d) \text{ für } n \geq 2 \text{ und } d \leq n - 1,$$

(iv) (Erweiterung des Alphabets)
$$A_q(n, d) \leq A_{q+1}(n, d).$$

Zum Beweis der Ableitung verwende man $J := K$ und $R_j := \{v \in K^n \mid v_n = j\}$, in den anderen Fällen $|J| = 1$. Zudem nutze man $\varphi : v \mapsto (v, y)$ für ein festes $y \in K$ bzw. $v \mapsto (v_1, v_2, ..., v_{n-1})$ bzw. $v \mapsto v$.

In Lee-Räumen zeigt man analog:

(i) (Verlängerung)
$$A_q^L(n, d) \leq A_q^L(n + 1, d),$$

(ii) (Ableitung)
$$\frac{A_q^L(n, d)}{q} \leq A_q^L(n - 1, d) \text{ für } n \geq 2 \text{ und } d \leq (n - 1) \left\lfloor \frac{q}{2} \right\rfloor,$$

(iii) (Erweiterung des Alphabets)

$$A_q^L(n,d) \leq A_{q+1}^L(n,d).$$

In Hamming-Permutationsräumen gilt, vgl. Quistorff [47]:

(i) (Verlängerung)

$$A_n(d) \leq A_{n+1}(d),$$

(ii) (Modifizierte Punktierung)

$$A_n(d) \leq A_{n-1}(d-3) \text{ für } d \geq 5 \text{ und } A_n(4) \leq A_{n-1}(2),$$

(iii) (Ableitung)

$$\frac{A_n(d)}{n} \leq A_{n-1}(d) \text{ für } n \geq 3 \text{ und } d \leq n-1,$$

Im Johnson-Raum gilt $k|C| = \sum_{x=1}^n |\{v \in C \mid v_x = 1\}| \leq nA(n-1, 2e, k-1)\,\forall C \subseteq J_{k,n}$, woraus eine der Ableitung nicht unähnliche Schranke folgt.

Satz 5.2 *In $(J_{k,n}, d_J)$ gilt*

$$A(n,2e,k) \leq \frac{n}{k} A(n-1, 2e, k-1)$$

und damit $A(n,2k,k) \leq \frac{n}{k}$ *sowie* $A(n,2e,k) \leq \frac{n}{k}\left\lfloor \frac{n-1}{k-1} \left\lfloor \dots \left\lfloor \frac{n-k+e}{e} \right\rfloor \dots \right\rfloor \right\rfloor$.

Hilfreich für überdeckende Mengen ist folgende Aussage.

Lemma 5.3 *Sei $\varphi : R \to \bar{R}$ eine surjektive Abbildung. Setze*

$$M := \{(d^R(v,w), d^{\bar{R}}(\varphi(v), \varphi(w))) \in D(R) \times D(\bar{R}) \mid v, w \in R\}.$$

Zu $e \in D(R)$ setze $M_e := \{\bar{e} \in D(\bar{R}) \mid (e, \bar{e}) \in M\}$ und $\Omega(e) := \max \bigcup_{\tilde{e} \leq e} M_{\tilde{e}} \in D(\bar{R})$. Dann gilt

$$\gamma(e) \geq \bar{\gamma}(\Omega(e)).$$

Beweis: Sei $C \subseteq R$ eine e-überdeckende Menge mit $|C| = \gamma(e)$. Ist $\bar{w} \in \bar{R}$, so existiert ein $w \in R$ mit $\varphi(w) = \bar{w}$ und ein $v \in C$ mit $d^R(v, w) \leq e$. Damit folgt $d^R(\varphi(v), \bar{w}) \leq \Omega(e)$, d.h. $\varphi(C)$ ist $\Omega(e)$-überdeckend mit $\gamma(e) = |C| \geq |\gamma(C)| \geq \gamma(\Omega(e))$. □

Eine Anwendung in Hamming-Räumen ist die Punktierung $K_q(n, e) \geq K_q(n-1, e)$ für $n > e$.

Es folgen nun einige induzierte Schranken, bei denen jeweils drei endliche metrische Räume involviert sind.

(i) (Direkte Produkte) Sei $R = K^n$, $R' = K'^n$, $\bar{R} = (K \times K')^n$ und $d^R = d^{R'} = d^{\bar{R}} = d_H$. Dann ist

$$\varphi : R \times R' \to \bar{R}, (v, v') \mapsto ((v_1, v_1'), (v_2, v_2'), ..., (v_n, v_n'))$$

eine Bijektion. Ist zudem sowohl $C \subseteq R$ als auch $C' \subseteq R'$ eine e-unabhängige Menge, so trifft dies auch auf $\varphi(C \times C')$ zu. Damit gilt

$$A_q(n, d) \cdot A_{q'}(n, d) \leq A_{qq'}(n, d).$$

Für eine Variante in Lee-Räumen mit $\varphi : (v, v') \mapsto qv' + v$ vgl. Racsmány [52]. Eine andere Variante in Hamming-Räumen führt auf

$$q^{n-1} K_{q'}(n, 1) \geq K_{qq'}(n, 1),$$

vgl. Cohen et al. [17].

(ii) (Verkettungen) Sei $R = K^n$, $R' = K^{n'}$, $\bar{R} = R \times R' = K^{n+n'}$ und $d^R = d^{R'} = d^{\bar{R}} = d_H$. Ist $C = \{v^{(j)} \in R \mid j \in J\}$ eine e-unabhängige und $C' = \{w^{(j)} \in R' \mid j \in J'\}$ eine e'-unabhängige Menge, so ist $\{(v^{(j)}, w^{(j)}) \in \bar{R} \mid j \in J \cap J'\}$ eine $(e + e' + 1)$-unabhängige Menge. Damit gilt

$$\min\{A_q(n, d), A_q(n', d')\} \leq A_q(n + n', d + d').$$

Eine andere Variante liefert $A_q(n, d) \leq A_{q'}(n \cdot n', d \cdot d')$, sofern $q \leq A_{q'}(n', d')$, vgl. Dumer [23]. Ist C eine e-überdeckende und C' eine e'-überdeckende Menge, so ist $C \times C'$ eine $(e + e')$-überdeckende Menge. Damit gilt

$$K_q(n, e) \cdot K_q(n', e') \geq K_q(n + n', e + e').$$

Hieraus folgt insbesondere $K_q(n,e) \geq K_q(n+1,e+1)$ und $qK_q(n,e) \geq K_q(n+1,e)$. In einem anderen Spezialfall führt eine Verbesserung auf $2^n K_2(n,1) \geq K_2(2n+1,1)$, vgl. Cohen et al. [17]. Verkettungen sind auch in Lee-Räumen und Hamming-Permutationsräumen möglich.

In Spezialfällen gibt es induzierte Schranken, in denen die Kardinalitäten $\gamma(e)$ und $\beta(e')$ gemeinsam auftreten, vgl. Cohen et al. [17].

5.2 Konstruktive Schranken

Für den folgenden Satz wird die Distanzinvarianz noch etwas abgeschwächt.

Satz 5.4 *Es existiere V_e.*

(i) (Gilbert-Schranke)

$$\beta(e) \geq \frac{|R|}{V_e}.$$

(ii)

$$\gamma(e) \leq |R| \frac{1 + \ln V_e}{V_e}.$$

Zum Beweis von (i) beachte man, dass sich für jedes $j \in J := \left\{1, 2, ..., \left\lceil \frac{|R|}{V_e} \right\rceil \right\}$ ein $v^{(j)} \in R \setminus \bigcup_{x=1}^{j-1} B_e(v^{(x)})$ auswählen lässt, da $j - 1 < \left\lceil \frac{|R|}{V_e} \right\rceil$ und somit $|R \setminus \bigcup_{x=1}^{j-1} B_e(v^{(x)})| \geq |R| - (j-1)V_e > 0$. Die Gilbert-Schranke kann auf die duale Version des graphentheoretischen Satzes von Turán zurückgeführt werden, vgl. Jukna [32]. Im Fall $(R, d^R) = ((\mathrm{GF}(q))^n, d_H)$ existiert zudem als Variante eine modifizierte Gilbert-Schranke, deren Verschärfung wiederum die Varšamov-Schranke ist, vgl. etwa Heise/Quattrocchi [29]. Zum Beweis von (ii) vgl. ebenfalls Jukna [32].

In Spezialfällen gibt es viele weitere konstruktive Schranken, insbesondere für $A_q(n,d)$ und $K_q(n,e)$.

5.3 Destruktive Schranken

Eine Menge $C \subseteq R$ mit $\Delta(C) \leq e$ heißt *e-Antimenge*, im Sequenzraum auch *e-Anticode*. Ist $R = \biguplus_{j \in J} R_j$ eine Zerlegung in e-Antimengen, so gilt $\beta(e) \leq |J|$, vgl. auch Bode/Harborth [6].

Satz 5.5 (Code-Anticode-Schranke) *Sei* (R, d^R) *ein translationsinvarianter oder distanzregulärer endlicher metrischer Raum. Sind* $C, C' \subseteq R$ *mit* $D^*(C) \cap D^*(C') = \emptyset$, *so gilt*

$$|C| \cdot |C'| \leq |R|.$$

Ist C *eine* e*-Antimenge, so gilt*

$$\beta(e) \leq \frac{|R|}{|C|}.$$

Der aufwendige Beweis im distanzregulären Fall findet sich in Delsarte [21] und van Lint/Wilson [38]. Vgl. auch Ahlswede/Aydinian/Khachatrian [1]. Zum Beweis im translationsinvarianten Fall gemäß Frankl/Deza [25] seien $v, w \in C$ und $v', w' \in C'$ mit $v \circ v' = w \circ w'$. Dann gilt $d^R(v, w) = d^R(v \circ v', w \circ v') = d^R(w \circ w', w \circ v') = d^R(w', v') \in D(C) \cap D(C')$, also $v = w$ und $v' = w'$. Damit ist $|C| \cdot |C'| = |C \circ C'| \leq |R|$. □

Die Code-Anticode-Schranke motiviert die Suche nach (möglichst großen) e-Antimengen. Man betrachte einen Hamming-Raum oder einen Hamming-Permutationsraum, d.h. (R, d_H) mit $R \in \{K^n, \mathbf{S}_n\}$ für $n \in \mathbf{N}$. (Zur Vermeidung formaler Komplikationen im Hamming-Permutationsraum definiere man hier zusätzlich zu $B_j(v)$ und V_j für $j \in \{0, 2, 3, ..., n\}$ noch $B_1(v) := B_0(v) = \{v\}$ und $V_1 := V_0 = 1$.) Setze

$$I_k(v, w) := \{x \in \{1, 2, ..., k\} \mid v_x \neq w_x\}$$

für $k \in \{0, 1, ..., n\}$ und $v, w \in R$. Setze weiter

$$F_k(n) := |\{v \in R \mid \{1, 2, ..., k\} = I_k(v, w)\}|$$

für $k \in \{0, 1, ..., n\}$.

Satz 5.6 *Sei* $n \in \mathbf{N}$ *und* $R \in \{K^n, \mathbf{S}_n\}$. *Wenn* $e \in D(R)$ *und* $j \in \{0, 1, ..., \lfloor \frac{e}{2} \rfloor\}$ *sowie* $w \in R$, *dann ist*

$$C_e^{(j)}(w) := \{v \in R \mid j \geq |I_{n-e+2j}(v, w)|\} \supseteq B_j(w)$$

eine e*-Antimenge mit*

$$|C_e^{(j)}(w)| = \sum_{k=0}^{j} \binom{n-e+2j}{k} F_k(e - 2j + k) \geq V_j.$$

Ist e gerade, so gilt $C_e^{(\frac{e}{2})}(w) = B_{\frac{e}{2}}(w)$ *und damit* $|C_e^{(\frac{e}{2})}(w)| = V_{\frac{e}{2}}$. *Andernfalls gilt*

$$C_e^{(\frac{e-1}{2})}(w) = \left\{ v \in R \;\middle|\; \frac{e-1}{2} \geq |I_n(v,w)| \right\} \uplus$$
$$\uplus \left\{ v \in R \;\middle|\; \frac{e-1}{2} = |I_{n-1}(v,w)| \text{ und } v_n \neq w_n \right\}$$

und damit

$$\begin{aligned} \left| C_e^{(\frac{e-1}{2})}(w) \right| &= \left(\sum_{k=0}^{\frac{e-1}{2}} \binom{n}{k} F_k(k) \right) + \binom{n-1}{\frac{e-1}{2}} F_{\frac{e+1}{2}} \left(\frac{e+1}{2} \right) \\ &= V_{\frac{e-1}{2}} + \binom{n-1}{\frac{e-1}{2}} F_{\frac{e+1}{2}} \left(\frac{e+1}{2} \right). \end{aligned}$$

Im Fall $R = K^n$ *gilt* $F_k(n) = (q-1)^k q^{n-k}$ *und*

$$C_e^{(j)}(w) = B_j((w_1, w_2, ..., w_{n-e+2j})) \times K^{e-2j}.$$

Im Fall $R = \mathbf{S}_n$ *gilt* $F_k(n) = \sum_{x=0}^{k} (-1)^x \binom{k}{x} (n-x)!$.

Der Nachweis der Formel für $F_k(n)$ im Fall $R = \mathbf{S}_n$ erfolgt durch Induktion nach k. Alle anderen Aussagen sind direkt einsichtig.

Setzt man im Fall $R = K^n$ zudem

$$j := \begin{cases} \left\lfloor \frac{e}{2} \right\rfloor, & \text{falls } (e+1)q \leq 2n, \\ \left\lfloor \frac{n-e-2}{q-2} \right\rfloor, & \text{falls } (e+1)q > 2n \text{ und } n > e+1, \\ 0, & \text{falls } (e+1)q > 2n \text{ und } n \leq e+1, \end{cases}$$

so ist $C_e^{(j)}(w)$ ein e-Anticode größter Kardinalität, vgl. Ahlswede/Khachatrian [2]. Daher sind beispielsweise die Abschätzungen

$$A_4(10,5) \leq \left\lfloor \frac{|K^{10}|}{|C_4^{(2)}(w)|} \right\rfloor = \left\lfloor \frac{4^{10}}{436} \right\rfloor = 2404$$

sowie

$$A_4(8,5) \leq \left\lfloor \frac{|K^{8}|}{|C_4^{(1)}(w)|} \right\rfloor = \left\lfloor \frac{4^{8}}{304} \right\rfloor = 215$$

und

$$A_4(6,5) \le \left\lfloor \frac{|K^6|}{|C_4^{(0)}(w)|} \right\rfloor = \left\lfloor \frac{4^6}{4^4} \right\rfloor = 16$$

die besten Resultate, die in diesen Fällen aus der Code-Anticode-Schranke gewonnen werden können.

Im Hamming-Permutationsraum gilt beispielsweise

$$A_{10}(6) \le \left\lfloor \frac{|s_{10}|}{|C_5^{(1)}(w)|} \right\rfloor = \left\lfloor \frac{10!}{132} \right\rfloor = 27490,$$

während $|C_5^{(0)}(w)| = 120$ und $|C_5^{(2)}(w)| = 118$ schlechtere Resultate implizieren.

Die Code-Anticode-Schranke impliziert bei Verwendung von $C_e^{(0)}(w)$ folgende Abschätzung.

Satz 5.7 ((Joshi-)Singleton-Schranke) *In Hamming-Räumen und Hamming-Permutationsräumen gilt*

$$\beta(e) \le q^{n-e} \text{ bzw. } \beta(e) \le \frac{n!}{e!}.$$

Für Verallgemeinerungen in Sequenzräumen vgl. Răduică [53].

In vielen Fällen ist $\beta(e) \neq q^{n-e}$ bzw. $\beta(e) \neq \frac{n!}{e!}$ bekannt. Zudem gilt grundsätzlich $\beta(e) \neq q^{n-e} - 1$ bzw. $\beta(e) \neq \frac{n!}{e!} - 1$, vgl. Quistorff [47]. Für weitere Verbesserungen in Einzelfällen vgl. Quistorff [51].

Leicht einsichtig sind folgende Schranken.

Satz 5.8 (Kugelschranken)

(i) (Kugelpackungsschranke oder Hamming-Schranke) *Sofern $V_{r(\psi(e))}$ existiert, gilt*

$$\beta(e) \le \frac{|R|}{V_{r(\psi(e))}}.$$

(ii) (Kugelüberdeckungsschranke) *Sofern V_e existiert, gilt*

$$\gamma(e) \ge \frac{|R|}{V_e}.$$

Beweis: Für jede e-unabhängige Menge C ist nach Lemma 2.7 die Vereinigung $\bigcup_{v\in C} B_{r(\psi(e))}(v) \subseteq R$ disjunkt, d.h. $|C|V_{r(\psi(e))} \leq |R|$. Für jede e-überdeckende Menge C gilt $|C|V_e \geq |\bigcup_{v\in C} B_e(v)| = |R|$. □

Aus der Existenz von $V_{r(\psi(e))}$ folgt damit $\beta(e) \leq \gamma(r(\psi(e)))$. Liegt Translationsinvarianz oder Distanzregularität vor, so folgt die Kugelpackungsschranke aus der Code-Anticode-Schranke, da $\Delta(B_{r(\psi(e))}(v)) \leq e$.

Da im Fall $r(e) = r(\psi(e))$ die Kugelpackungsschranke für $\beta(e)$ häufig relativ schwach ist, betrachte man folgende Verallgemeinerung. Existiert zu jedem $v \in R$ eine Menge $P_e(v) \subseteq R$ mit $P_e(v) \cap P_e(w) = \emptyset \, \forall v, w \in R$ mit $d^R(v, w) > e$, so nennt man diese Mengen *verallgemeinerten Kugeln* bezüglich e. Sofern $|P_e(v)|$ für festes e unabhängig von v ist, setze $W_e := |P_e(v)|$. Dann folgt

$$\beta(e) \leq \frac{|R|}{W_e}. \tag{1}$$

Unter geeigneten Voraussetzungen gilt hierbei $\Delta(P_e(v)) \leq e$, so dass diese Schranke dann bei Vorliegen von Translationsinvarianz oder Distanzregularität ebenfalls eine Folgerung der Code-Anticode-Schranke ist. Geeignete Voraussetzungen im obigen Sinne sind: $\forall v, v' \in R \, \exists$ Autometrie $\varphi \, \forall w \in R$ gilt $\varphi(v) = v'$, $\varphi(P_e(w)) = P_e(\varphi(w))$ und $d^R(w, \varphi(w)) = d^R(v, v')$.

Beispielsweise sind für ungerades e in Hamming-Räumen und Hamming-Permutationsräumen die Mengen $P_e(v) := C_e^{(\frac{e-1}{2})}(v)$ verallgemeinerte Kugeln bezüglich e und es gilt $W_e := V_{\frac{e-1}{2}} + \binom{n-1}{\frac{e-1}{2}} F_{\frac{e+1}{2}} \binom{e+1}{2}$, vgl. Satz 5.6. In Lee-Räumen sind für ungerades e die Mengen $P_e(v) := B_{\frac{e-1}{2}}(v) + \{(0, 0, ..., 0, 0), (0, 0, ..., 0, 1)\}$ verallgemeinerte Kugeln bezüglich e.

Es gibt jedoch auch endliche metrische Räume mit folgenden Eigenschaften: Aufgrund fehlender Translationsinvarianz und Distanzregularität ist die Code-Anticode-Schranke nicht anwendbar. Für festes $e \in D(R)$ existieren neben $V_{r(\psi(e))}$ verallgemeinerte Kugeln bezüglich e mit $W_e > V_{r(\psi(e))}$. Hier verbessert (1) die Kugelpackungsschranke. Ein derartiges, durch einen Graphen induziertes Beispiel mit $|R| = 8$, $\beta(e) = 3$, $W_1 = 2 > 1 = V_0$, in dem sogar eine dreielementige 1-Antimenge existiert, lässt sich leicht konstruieren, vgl. auch van Lint/Wilson [38].

Zur Verbesserung der Kugelpackungsschranke $A_2(n,2e+1) \leq \frac{2^n}{V_e}$ und der Schranke

$$A_q(n,2e) \leq \frac{q^n}{V_{e-1} + \frac{\binom{n}{e}(q-1)^e}{\frac{n}{e}}}$$

gemäß (1) dient folgender Satz, vgl. Johnson [31], Vaessens/Aarts/van Lint [59].

Satz 5.9 (i) (Johnson-Schranke)

$$A_2(n,2e+1) \leq \frac{2^n}{V_e + \frac{\binom{n}{e+1} - \binom{2e+1}{e} A(n,2e+2,2e+1)}{\left\lfloor \frac{n}{e+1} \right\rfloor}}.$$

(ii)

$$A_q(n,2e) \leq \frac{q^n}{V_{e-1} + \frac{\binom{n}{e}(q-1)^e}{\left\lfloor \frac{n}{e} \right\rfloor}}.$$

Beweis: (i) Sei $C \subseteq R$ ein $(2e)$-unabhängiger Code in $(R, d^R) = (\{0,1\}^n, d_H)$. Setze $E := \{v \in R \mid d(v,C) = e+1\}$ und $F := \{(v,w) \in E \times C \mid d_H(v,w) = e+1\}$. Einerseits ist

$$|F| = \sum_{v \in E} |C \cap S_{e+1}(v)| \leq |E| A(n, 2e+2, e+1) = |E| \left\lfloor \frac{n}{e+1} \right\rfloor,$$

da $S_{e+1}(0,0,...,0) \subseteq J_{e+1,n}$. Andererseits gilt

$$\begin{aligned}
|F| &= \sum_{w \in C} \left| S_{e+1}(w) \setminus \bigcup_{w' \in C} B_e(w') \right| \\
&= \sum_{w \in C} \left| S_{e+1}(w) \setminus \bigcup_{w' \in C \cap S_{2e+1}(w)} (S_{e+1}(w) \cap S_e(w')) \right| \\
&\geq \sum_{w \in C} \left(|S_{e+1}(w)| - \sum_{w' \in C \cap S_{2e+1}(w)} |(S_{e+1}(w) \cap S_e(w'))| \right) \\
&\geq |C| \left(\binom{n}{e+1} - A(n,2e+2,2e+1) \binom{2e+1}{e} \right),
\end{aligned}$$

da $S_{2e+1}(0,0,...,0) \subseteq J_{2e+1,n}$. In Analogie zum Beweis der Kugelpackungsschranke ist $2^n \geq |C|V_e + |E|$.
(ii) Sei $C \subseteq R$ ein $(2e-1)$-unabhängiger Code in $(R, d^R) = (K^n, d_H)$. Setze $E := \{v \in R \mid d(v,C) = e\}$ und $F := \{(v,w) \in E \times C \mid d_H(v,w) = e\}$. Dann gilt $|F| = \sum_{v \in E} |C \cap S_e(v)| \leq |E| \left\lfloor \frac{n}{e} \right\rfloor$ und $|F| = \sum_{w \in C} |S_e(w)| = |C|\binom{n}{e}(q-1)^e$ sowie $q^n \geq |C|V_{e-1} + |E|$. □

Auch durch Untersuchung des *Exzesses* $(\sum_{v \in C} |B_e(v) \cap C'|) - |\bigcup_{v \in C} B_e(v) \cap C'|$ bzw. des *Defektes* $|C'| - \sum_{v \in C} |B_e(v) \cap C'|$ für geeignete $C' \subseteq R$ kann die Kugelüberdeckungs- bzw. Kugelpackungsschranke verbessert werden, vgl. van Wee [60]. Des weiteren können beide Kugelschranken und auch (1) durch eine geeignete Zerlegung $R = \biguplus_{j \in J} R_j$ verbessert werden, vgl. Quistorff [49].

Für die nachfolgende Schranke sei (K, d^K) ein endlicher metrischer Raum und $n \in \mathbf{N}$. Dann ist (R, d^R) mit $R = K^n$ und $d^R(v,w) = \sum_{x=1}^n d^K(v_x, w_x)$ ein Sequenzraum. Verwende

$$P_{(K,d^K)}(u) := \max \left\{ \sum_{\{j,k\} \subseteq \{0,1,...,u-1\}} d^K(v^{(j)}, v^{(k)}) \,\middle|\, (v^{(0)}, v^{(1)}, ..., v^{(u-1)}) \in K^u \right\}.$$

Satz 5.10 (Plotkin-Schranke) *Ist $e < \Delta(R)$, so impliziert $\beta(e) \geq u \in \mathbf{N} \setminus \{1\}$ die Abschätzung*

$$\psi(e)\binom{u}{2} \leq nP_{(K,d^K)}(u).$$

Beweis: Sei C ein e-unabhängiger Code mit $|C| = u$. Dann gilt $\psi(e)\binom{u}{2} \leq \sum_{\{v,w\} \subseteq C} d^R(v,w) \leq nP_{(K,d^K)}(u)$. □

Es gilt $P_{(K,d_H)}(u) = \sum_{j=0}^{q-2} \sum_{k=j+1}^{q-1} \lfloor \frac{u+j}{q} \rfloor \cdot \lfloor \frac{u+k}{q} \rfloor$. Zudem ist $P_{(\mathbf{Z}/q\mathbf{Z}, d_L)}(u)$ in vielen Fällen bekannt und in allen anderen relativ gut abgeschätzt. Vgl. Bogdanova et al. [7], Quistorff [50] und deren Referenzen.

In Hamming-Räumen existieren viele weitere destruktive Schranken, beispielsweise die durch lineare Programmierung gewonnenen und im Zusammenhang mit Association Schemes stehende Delsarte-Schranke für $\beta(e)$, vgl. Delsarte [20], van Lint [37], die Schranke $\gamma(1) \geq \frac{q^{n-1}}{n-1}$ für $n \geq 2$, vgl. Kalbfleisch/Weiland [33], Rodemich [54], Quistorff [48], sowie eine untere Schranke für $i(1)$, vgl. Quistorff [46].

Auch in gemischten Hamming-Räumem, Lee-Räumen und Hamming-Permutationsräumen gibt es Schranken für $\beta(e)$, die im Zusammenhang mit

Association Schemes und sogenannten Product Schemes stehen, vgl. Brouwer et al. [12], Tarnanen [57], [58].

6 Ausgezeichnete Mengen

Mengen, deren Kardinalität eine der erwähnten destruktiven Schranken mit Gleichheit erfüllen, haben oftmals besondere Eigenschaften. Von trivialen Fällen abgesehen sind diese so ausgezeichneten Mengen in der Regel selten.

(i) Sei $C \subseteq R$ eine e-unabhängige Menge in einem translationsinvarianten oder distanzregulären endlichen metrischen Raum. Falls es eine e-Antimenge $C' \subseteq R$ mit $|C| \cdot |C'| = R$ gibt, so heißt C eine *e-Durchmesser-perfekte Menge*, vgl. Ahlswede/Aydinian/Khachatrian [1].

(ii) Sei $C \subseteq K^n$ bzw. $C \subseteq \mathbf{S}_n$ eine e-unabhängige Menge in einem Hamming-Raum bzw. Hamming-Permuationsraum. Gilt $|C| = q^{n-e}$ bzw. $|C| = \frac{n!}{e!}$, so heißt C ein *MDS-Code (Maximum Distance Seperable Code)* bzw. eine *mehrfach scharf transitive Permutationsmenge (MST-Permutationsmenge)*. Genauer spricht man von einem q-nären $(n, n-e)$-MDS-Code bzw. einer $(n-e)$-fach scharf transitiven Permutationsmenge vom Grad n. Charakterisiert ist C durch die Bedingung, dass zu paarweise verschiedenen $x_1, x_2, ..., x_{n-e} \in \{1, 2, ..., n\}$, und zu $y_1, y_2, ..., y_{n-e}$ aus K bzw. paarweise verschieden aus $\{1, 2, ..., n\}$ genau ein $v \in C$ mit $v_{x_1} = y_1$, $v_{x_2} = y_2$, ..., $v_{x_{n-e}} = y_{n-e}$ existiert. MDS-Codes und MST-Permutationsmengen werden in Quistorff [47], Bonisoli/Quattrocchi [9] sowie ihren Referenzen diskutiert, sie sind e-Durchmesser-perfekt. Ihre Existenz ist in Hamming-Räumen für $e \in \{0, 1, n-1\} \cap D(R)$, in Hamming-Permutationsräumen für $e \in \{0, 2, n-1\} \cap D(R)$ trivial. Bei großzügigem Umgang mit den Definitionen trifft Letzteres auch auf $e = 1$ zu.

(iii) Sei $e \in D(R)$. Eine Menge $C \subseteq R$ heißt genau dann *e-perfekt*, wenn

$$\biguplus_{v \in C} B_e(v) = R.$$

Falls V_e existiert, so gilt: C ist e-perfekt $\Leftrightarrow$ C ist e-überdeckend mit $|C| = \frac{|R|}{V_e}$.

Sei $\tilde{e} \in D(R) \setminus \{\Delta(R)\}$. Setze $e := r(\psi(\tilde{e}))$. Falls V_e existiert, so gilt: C ist $\tilde{e}$-unabhängig mit $|C| = \frac{|R|}{V_e} \Rightarrow C$ ist e-perfekt.

Sei $\tilde{e} \in D(R) \setminus \{\Delta(R)\}$. Setze $e := r(\psi(\tilde{e}))$. Sei $e' \in D(R)$ mit $e \leq e' \leq \tilde{e}$. Falls $\Delta(R) > 2e$ und $\psi(\tilde{e}) \leq \min\{\bar{e} \mid \bar{e} > 2e\}$, falls die Existenz von Zwischenwerten und von V_e gesichert ist, dann gilt: C ist e-perfekt $\Rightarrow$ C ist $\tilde{e}$-unabhängig mit $|C| = \frac{|R|}{V_e}$ und zudem maximal e'-unabhängig. Liegt darüber hinaus auch noch Translationsinvarianz oder Distanzregularität vor, so ist C auch $\tilde{e}$-Durchmesser-perfekt.

Gilt $r(d(C)) = t(C) =: e$, so ist C eine e-perfekte Menge. Falls die Existenz von Zwischenwerten gewährleistet ist, so gilt auch die Umkehrung.

Falls V_e existiert, so gilt: Es existiert eine e-perfekte Menge $\Leftrightarrow \gamma(e) = \frac{|R|}{V_e}$.

Sei $\tilde{e} \in D(R) \setminus \{\Delta(R)\}$. Setze $e := r(\psi(\tilde{e}))$. Dann gilt: $\beta(\tilde{e}) = \frac{|R|}{V_e} \Leftrightarrow$ es existiert eine e-perfekte Menge $\Rightarrow i(e) = \frac{|R|}{V_e}$.

Sei (R, d^R) ein graphischer Raum. Im Fall $\tilde{e} = 2e \in D(R) \setminus \{\Delta(R)\}$ gerade ist dann $r(\psi(\tilde{e})) = \frac{\tilde{e}}{2} = e$. Existiert zudem V_e, so gilt:

$$
\begin{aligned}
C \text{ ist } e\text{-perfekt} \quad &\Leftrightarrow \quad C \text{ ist } e\text{-überdeckend mit } |C| = \frac{|R|}{V_e} \\
&\Leftrightarrow \quad C \text{ ist } \tilde{e}\text{-unabhängig mit } |C| = \frac{|R|}{V_e} \\
&\Leftrightarrow \quad r(d(C)) = t(C) = e \\
&\Rightarrow \quad \gamma(e) = i(e) = \beta(\tilde{e}) = \frac{|R|}{V_e}.
\end{aligned}
$$

Existenzprobleme für perfekte Mengen sind in vielen endlichen metrischen Räumen diskutiert worden, vgl. etwa Cohen et al. [17], Astola [4], Deza/Huang [22], Solé [56].

(iv) Sei C ein e-unabhängiger Code mit $|C| \geq 2$ in einem Sequenzraum (R, d^R) mit $R = K^n$ und $d^R(v,w) = \sum_{x=1}^{n} d^K(v_x, w_x)$. Setze $e' := nP_{(K,d^K)}(|C|)\binom{|C|}{2}^{-1} \in \mathbf{Q}$. Im Fall $\psi(e) = e'$ gilt $D^*(C) = \{e'\}$ und C heißt *e'-äquidistanter* Code. Vgl. auch Semakov/Zinov'ev [55], Bogdanova et al. [7].

7 Tabellen

Für einige Klassen endlicher metrischer Räume existieren Tabellen mit oberen und/oder unteren Schranken für $\beta(e)$ oder $\gamma(e)$.

(i) Hamming-Räume: Tabellen für $\gamma(e)$ in Cohen et al. [17], im Fall $q = 2$ auch in Litsyn [41]. Tabellen für $\beta(e)$ mit $q \leq 6$ in Litsyn [39], [40], Brouwer et al. [12], [13], Bogdanova et al. [7], [8], Quistorff [47].

(ii) Gemischte Hamming-Räume: Tabellen für $\gamma(e)$ in Cohen et al. [17], für $\beta(e)$ in Brouwer et al. [12].

(iii) Hamming-Permutationsräume: Tabellen für $\beta(e)$ in Quistorff [47].

(iv) Johnson-Räume: Tabellen für $\gamma(e)$ in Li/van Rees [36] und Li [35]. Tabellen für $\beta(e)$ in Brouwer et al. [13].

Zudem sind für Schachbrettprobleme Resultate hinsichtlich $ir(e)$, $\gamma(e)$, $i(e)$, $\beta(e)$, $\Gamma(e)$, $IR(e)$, insbesondere für $R = K^2$ und $e = 1$, tabelliert worden, vgl. Fricke et al. [26] und deren Referenzen.

Literatur

[1] Ahlswede, R. / Aydinian, H.K. / Khachatrian, L.H.: On Perfect Codes and Related Concepts, *Des. Codes Cryptogr.*, 22 (2001), 221-237.

[2] Ahlswede, R. / Khachatrian, L.H.: The Diametric Theorem in Hamming Spaces - Optimal Anticodes, *Adv. Appl. Math.*, 20 (1998), 429-449.

[3] Allison, L. / Yee, C.N. / McGaughey, M.: Three Dimensional Queen Problems, *Technical Report* 89/130, Monash Univ., 1988, `http://www.csse.monash.edu.au/~lloyd/tildeAlgDS/Recn/Queens3D/`.

[4] Astola, J.: On Perfect Codes in the Lee-Metric, *Ann. Univ. Turku., Ser. A I*, 176 (1978).

[5] Blokhuis, A. / Egner, S. / Hollmann, H.D.L. / van Lint, J.H.: On Codes with Covering Radius 1 and Minimum Distance 2, eingereicht.

[6] Bode, J.-P. / Harborth, H.: Independent Chess Pieces on Euclidean Bords, *J. Comb. Math. Comb. Comput.*, 33 (2000), 209-223.

[7] Bogdanova, G.T. / Brouwer, A.E. / Kapralov, S.N. / Östergård, P.R.J.: Error-Correcting Codes over an Alphabet of Four Elements, *Des. Codes Cryptogr.*, 23 (2001), 333-342.

[8] Bogdanova, G.T. / Östergård, P.R.J.: Bounds on Codes over an Alphabet of Five Elements, *Discr. Math.*, 240 (2001), 13-19.

[9] Bonisoli, A. / Quattrocchi, P.: Existence and Extension of Sharply k-Transitive Permutation Sets: A Survey and some New Results, *Ars Comb.*, 24A (1987), 163-173.

[10] Brightwell, G. / Katona, G.O.H.: A New Type of Coding Problem, *Stud. Sc. Math. Hung.*, 38 (2001), 139-147.

[11] Brouwer, A.E. / Cohen, A.M. / Neumaier, A.: *Distance-Regular Graphs*, Springer, Berlin, 1989.

[12] Brouwer, A.E. / Hämäläinen, H.O. / Östergård, P.R.J. / Sloane, N.J.A.: Bounds on Mixed Binary/Ternary Codes, *IEEE Trans. Inform. Theory*, 44 (1998), 140-161.

[13] Brouwer, A.E. / Shearer, J.B. / Sloane, N.J.A. / Smith, W.D.: A New Table of Constant Weight Codes, *IEEE Trans. Inform. Theory*, 36 (1990), 1334-1380.

[14] Burger, A.P. / Mynhardt, C.M. / Cockayne, E.J.: Queen Graphs for Chessboards on the Torus, *Australas. J. Comb.* 24 (2001), 231-246.

[15] Camion, P.: Codes and Association Schemes: Basic Properties of Association Schemes Relevant to Coding, in: Pless, V.D. / Huffman, W.C. (eds.), *Handbook of Coding Theory, Vol. 2*, Elsevier, Amsterdam, 1998, 1441-1566.

[16] Cockayne, E.J. / Hedetniemi, S.T. / Miller, D.J.: Properties of Hereditary Hypergraphs and Middle Graphs, *Cand. Math. Bull.*, 21 (1978), 461-468.

[17] Cohen, G. / Honkala, I. / Litsyn, S. / Lobstein, A.: *Covering Codes*, North-Holland, Amsterdam, 1997.

[18] Colbourn, C.J.: Winning the Lottery, in: Colbourn, C.J. / Dinitz, J.H. (eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, New York, London, Tokyo, 1996, 578-584.

[19] Davydov, V.A.: Codes Correcting Errors in the Modulus Metric, Lee Metric, and Opertator Errors, *Problemy Peredachi Informatsii*, 29 (1993), 10-20. *Prob. Inform. Transmission*, 29 (1993), 209-217.

[20] Delsarte, P.: Bounds for Unrestricted Codes, by Linear Programming, *Philips Res. Rep.*, 27 (1972), 272-289.

[21] Delsarte, P.: An Algebraic Approach to the Association Schemes of Coding Theory, *Phillips Res. Rep. Suppl.*, 10 (1973).

[22] Deza, M. / Huang, T.: Metrics on Permutations, a Survey, *J. Comb. Inf. Sys. Sci.*, 23 (1998), 173-185.

[23] Dumer, I.: Concatenated Codes and Their Multilevel Generalizations, in: Pless, V.D. / Huffman, W.C. (eds.), *Handbook of Coding Theory, Vol. 2*, Elsevier, Amsterdam, 1998, 1911-1988.

[24] Enomoto, H. / Katona, G.O.H.: Pairs of Disjoint q-element Subsets far from each other, *Electr. J. Comb.*, 8 (2001), #R7.

[25] Frankl, P. / Deza, M.: On the Maximum Number of Permutations with Given Maximal or Minimal Distance, *J. Comb. Th., Ser. A*, 22 (1977), 352-360.

[26] Fricke, G.H. / Hedetniemi, S.M. / Hedetniemi, S.T. / McRae, A.A. / Wallis, C.K. / Jacobson, M.S. / Martin, H.W. / Weakley, W.D.: Combinatorial Problems on Chessboards: A Brief Survey, in: Alavi, Y. / Schwenk, A. (eds.), *Graph Theory, Combinatorics, and Applications, Vol. 1*, Wiley, New York, 1995, 507-528.

[27] Golomb, S.W. / Posner, E.C.: Rook Domains, Latin Squares, Affine Planes, and Error-Distributing Codes, *IEEE Trans. Inform. Theory*, 10 (1964), 196-208.

[28] Hedetniemi, S.T. / Lasker, R.C. (guesteds.): Topics on Domination, *Discr. Math., Special Volume*, 86 (1990).

[29] Heise, W. / Quattrocchi, P.: *Informations- und Codierungstheorie*, 3. Auflage, Springer, Berlin, Heidelberg, 1995.

[30] Jacobson, M.S. / Peters, K.: Chordal Graphs and Upper Irredundance, Upper Domination and Independence, *Discr. Math.*, 86 (1990), 59-69.

[31] Johnson, S.M.: A New Upper Bound for Error-Correcting Codes, *IRE Trans. Inform. Theory*, 8 (1962), 203-207.

[32] Jukna, S.: *Extremal Combinatorics*, Springer, Berlin, Heidelberg, New York, 2001.

[33] Kalbfleisch, J.G. / Weiland, P.H.: Some New Results for the Covering Problem, *Recent Prog. Comb., Proc. Third Waterloo Conf. 1968*, Academic Press, New York, 1969.

[34] Levenshtein, V.I.: Universal Bounds for Codes and Designs, in: Pless, V.D. / Huffman, W.C. (eds.), *Handbook of Coding Theory, Vol. 1*, Elsevier, Amsterdam, 1998, 499-648.

[35] Li, P.C.: Lotto Tables, `http:// www.cs.umanitoba.ca/~lipakc/lottotables.html`.

[36] Li, P.C. / van Rees, G.H.J.: Lotto Tables, *J. Comb. Des.*, 10 (2002), 335-359.

[37] van Lint, J.H.: *Introduction to Coding Theory*, Third Edition, Springer, Berlin, Heidelberg, New York, 1999.

[38] van Lint, J.H. / Wilson, R.M.: *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.

[39] Litsyn, S.: An Updated Table of the Best Binary Codes Known, in: Pless, V.D. / Huffman, W.C. (eds.), *Handbook of Coding Theory, Vol. 1*, Elsevier, Amsterdam, 1998, 463-498.

[40] Litsyn, S.: Table of Nonlinear Binary Codes, `http://www.eng.tau.ac.il/~litsyn/tableand/index.html`.

[41] Litsyn, S.: Table of the Best Currently Known Lower and Upper Bounds on the Smallest Size of a Covering Code, `http://www.eng.tau.ac.il/~litsyn/tablecr/index.html`.

[42] MacWilliams, F.J. / Sloane, N.J.A.: *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, New York, Oxford, 1977.

[43] Nordwest Lotto und Toto Hamburg (Hrsg.): *System-Broschüre für Lotto*, 1. Auflage, Hamburg, 2001.

[44] Östergård, P.R.J. / Quistorff, J. / Wassermann, A.: New Results on Codes with Covering Radius 1 and Minimum Distance 2, eingereicht.

[45] Pólya, G.: Über die doppelt-periodischen Lösungen des n-Damen-Problems, in: Ahrens, W. (Hrsg.): *Mathematische Unterhaltungen und Spiele, Band II*, Teubner, Stuttgart, 1918, 364-374.

[46] Quistorff, J.: On Full Partial Quasigroups of Finite Order and Local Cardinal Maximum Codes, *Beitr. Alg. Geom.*, 40 (1999), 495-502.

[47] Quistorff, J.: *Simultane Untersuchung mehrfach scharf transitiver Permutationsmengen und MDS-Codes unter Einbeziehung ihrer Substitute*, Habilitationsschrift, Univ. Hamburg, 1999. Shaker Verlag, Aachen, 2000.

[48] Quistorff, J.: On Codes with Given Minimum Distance and Covering Radius, *Beitr. Alg. Geom.*, 42 (2001), 601-611.

[49] Quistorff, J.: Improved Sphere Bounds in Finite Metric Spaces, eingereicht.

[50] Quistorff, J.: Some Remarks on the Plotkin Bound, eingereicht.

[51] Quistorff, J.: Slight Improvements of the Singleton Bound, eingereicht.

[52] Racsmány, A.: On Constructing Codes with Given Distance in Lee-Metric, *Prob. Contr. Inf. Th.*, 15 (1986), 377-384.

[53] Răduică, M.: Marginile Plotkin si Ioshi relativ la coduri arbitrar metrizate, *Bul. Univ. Braşov*, C 22 (1980), 115-120.

[54] Rodemich, E.R.: Coverings by Rook Domains, *J. Comb. Th.*, 9 (1970), 117-128.

[55] Semakov, N.V. / Zinov'ev, V.A.: Equidistant q-ary Codes with Maximal Distance and Resolvable Balanced Incomplete Block Designs, *Problemy Peredachi Informatsii*, 4 (1968), 3-10. *Prob. Inform. Transmission*, 4 (1968), 1-7.

[56] Solé, P.: A Lloyd Theorem in Weakly Metric Association Schemes, *Europ. J. Comb.*, 10 (1989), 189-196.

[57] Tarnanen, H.: Upper Bounds for Constant Weight Codes and Lee Codes Slightly outside the Plotkin Range, *Discrete Appl. Math.*, 16 (1987), 265-277.

[58] Tarnanen, H.: Upper Bounds on Permutation Codes via Linear Programming, *Europ. J. Comb.*, 20 (1999), 101-114.

[59] Vaessens, R.J.M. / Aarts, E.H.L. / van Lint, J.H.: Genetic Algorithms in Coding Theory - a Table for $A_3(n, d)$, *Discrete Appl. Math.*, 45 (1993), 71-87.

[60] van Wee, G.J.M.: Bounds on Packings and Coverings by Spheres in q-ary and Mixed Hamming Spaces, *J. Comb. Th., Ser. A*, 57 (1991), 117-129.

[61] Willems, W.: *Codierungstheorie*, Walter de Gruyter, Berlin, New York, 1999.