Bachelorarbeit

Über Assoziationsschemata und Codes

Lukas Klawuhn

Matrikelnummer: 175412

Fakultät für Mathematik
Technische Universität Dortmund
Abgabe: 13. Oktober 2017

betreut von Prof. Dr. Franz Kalhoff

Vorwort

Assoziationsschemata wurden erstmals ca. 1950 von Bose und Shimamoto als kombinatorische Objekte explizit definiert [3]. Tatsächlich ist die Struktur eines Assoziationsschemas auch schon in einem Artikel von Bose und Nair von 1939 zu erkennen, in dem sie sich mit *partially balanced incomplete block designs* beschäftigten [2]. Seit Assoziationsschemata Ende der 50er Jahre durch äquivalente Axiome auch als algebraische Objekte untersucht wurden, wurde mit ihnen in vielen mathematischen Bereichen wie etwa der Codierungstheorie gearbeitet und viele Probleme lassen sich auf natürliche Weise in die Theorie der Assoziationsschemata übersetzen.
Grob gesagt besteht ein Assoziationsschema aus einer endlichen Grundmenge X und einer Partition des kartesischen Produktes $X \times X$. Wenn die Partition einige besondere Axiome erfüllt, so spricht man von einem Assoziationsschema. Wegen der Ähnlichkeit dieser Axiome zu den Gruppenaxiomen wird die Theorie der Assoziationsschemata oft auch als "Gruppentheorie ohne Gruppen" bezeichnet. Beispiele sind:

- die oben genannten Designs in der Designtheorie
- distanzreguläre Graphen in der Graphentheorie
- besondere metrische Räume (dazu gehören insbesondere das Hamming- und das Johnson-Schema in der Codierungstheorie)
- eine endliche Gruppe mit ihren Konjugationsklassen
- die Menge der k-dimensionalen Untervektorräume von $\mathbb{F}_q^n$
- das Assoziationsschema von symmetrischen Bilinearformen über $\mathbb{F}_q$

Mit Letzterem werden wir uns in dieser Arbeit hauptsächlich beschäftigen.
Diese Arbeit soll eine Einführung in die Theorie der Assoziationsschemata geben und sie mit der Codierungstheorie verbinden. Dazu werden in Kapitel 1 die grundlegenden Begriffe definiert und an Beispielen verdeutlicht. Anschließend wird in Kapitel 2 das Assoziationsschema der symmetrischen Bilinearformen definiert und einige Eigenschaften werden angegeben. In Kapitel 3 gehen wir dann genauer auf Teilmengen in Assoziationsschemata und den Begriff des d-Codes ein und vergleichen ihn mit dem klassischen Codebegriff aus der Codierungstheorie. Schließlich benutzen wir die aufgestellte Theorie in Kapitel 4, um Schranken für d-Codes im Assoziationsschema der symmetrischen Bilinearformen herzuleiten. Zum Schluss wird ein kleiner Ausblick auf noch ungelöste Probleme gegeben, an denen weiter geforscht werden kann. Wir werden dabei sehen, dass sich das Finden von möglichst guten Codes, wie es in der Codierungstheorie betrieben

wird, direkt in die Theorie der Assoziationsschemata übersetzen lässt. Dort stehen uns dann weitere Methoden dafür zur Verfügung.
Natürlich ist es nicht möglich, die komplette Theorie in dieser Bachelorarbeit darzulegen. Es gibt viele weitere Begriffe sowie Möglichkeiten, Assoziationsschemata zu untersuchen, die in dieser Arbeit nicht genannt werden. Außerdem werden Beweise weggelassen, wenn sie zu komplex sind und den Rahmen dieser Arbeit sprengen würden, wenn sie zu weit vom Thema wegführen oder wenn sie zu viel Vorbereitung benötigen.

Inhaltsverzeichnis

1 Grundlagen

In diesem Kapitel definieren wir Assoziationsschemata und Begriffe, die zur Untersuchung nötig sind. Dazu werden lediglich Grundkenntnisse aus der linearen Algebra (siehe etwa das Buch von Beutelspacher [1]) benötigt.

1.1 Grundbegriffe

In diesem Abschnitt werden die Grundlagen der Theorie der Assoziationsschemata beschrieben. Dafür folgen wir der Arbeit "An algebraic approach to the association schemes of coding theory" von Delsarte [4] und Kapitel 21 des Buches "The Theory of Error-Correcting Codes " von MacWilliams und Sloane [10].

Definition. Sei $n \in \mathbb{N}_0$. Ein *Assoziationsschema* mit n Klassen ist ein Paar $(X, (R_i)_{i=0}^n)$ bestehend aus einer nichtleeren, endlichen Menge X mit $|X| \geq 2$ und nichtleeren Relationen $R_i \subseteq X \times X$, $i = 0, \ldots, n$, sodass gilt:

(A0) $\bigcup_{i=0}^{n} R_i = X \times X$ und $R_i \cap R_j = \emptyset$ für alle $i, j \in \{0, \ldots, n\}$ mit $i \neq j$, d.h. $(R_i)_{i=0}^n$ ist eine Partition von $X \times X$.

(A1) $R_0 = \{(x, x) \in X \times X \mid x \in X\}$, R_0 ist also die identische Relation.

(A2) Für jedes $i \in \{0, \ldots, n\}$ gibt es ein $j \in \{0, \ldots, n\}$, sodass $R_i^{-1} = R_j$. Dabei bezeichnet $R_i^{-1} = \{(y, x) \in X \times X \mid (x, y) \in R_i\}$ die zu R_i inverse Relation.

(A3) Es gilt für alle $i, j, k \in \{0, \ldots, n\}$: Für ein festes Paar $(x, y) \in R_k$ ist die Anzahl der $z \in X$, sodass $(x, z) \in R_i$ und $(z, y) \in R_j$ eine Konstante p_{ij}^k, die nur von i, j und k abhängt, nicht aber von der Wahl der Elemente x und y. Diese Zahlen heißen *Schnittzahlen* (engl. *intersection numbers*) des Assoziationsschemas.

Gilt $p_{ij}^k = p_{ji}^k$ für alle $i, j, k \in \{0, \ldots, n\}$, so heißt das Assoziationsschema *kommutativ*. Gilt $R_i^{-1} = R_i$ für alle $i \in \{0, \ldots, n\}$, so heißt das Assoziationsschema *symmetrisch*. Axiom (A2) definiert eine Involution $\sigma : \{0, \ldots, n\} \to \{0, \ldots, n\}$, $i \mapsto i^\sigma$, durch $R_{i^\sigma} = R_i^{-1}$. Bei einem symmetrischen Assoziationsschema ist σ also die Identität auf $\{0, \ldots, n\}$. Die Zahl $v_i := p_{ii^\sigma}^0$ heißt die *Valenz* (engl. *valency*) von R_i.

Im Folgenden bezeichnen wir mit R kurz das System der Relationen eines Assoziationsschemas, also $R := (R_i)_{i=0}^n$. Außerdem seien alle betrachteten Schemata kommutativ. Dies reicht aus, um die bekanntesten Assoziationsschemata zu untersuchen. Insbesondere sind alle in der Einleitung genannten Beispiele kommutativ. Einige Ergebnisse wie (1.3) und (1.4) gelten aber auch für beliebige Assoziationsschemata.

1.1 Beispiel. Aufgrund von Axiom (A1) und der Forderung $|X| \geq 2$ gibt es kein Assoziationsschema mit 0 Klassen. Denn R_0 enthielte nur die Paare der Form (x, x) mit $x \in X$, dies kann aber wegen $|X| \geq 2$ noch nicht ganz $X \times X$ sein. Wir betrachten also nun den Fall $n = 1$:
Es sei X eine beliebige endliche Menge mit mindestens 2 Elementen. Benötigt werden zwei Relationen R_0 und R_1, sodass R_0 und R_1 eine Partition von $X \times X$ bilden und dabei R_0 die identische Relation ist. Offenbar muss dann $R_1 = (X \times X) \setminus R_0$ gelten, also $R_1 = \{(x, y) \in X \times X \mid x \neq y\}$. Dann gelten (A0) und (A1), und wegen $R_0^{-1} = R_0$ und $R_1^{-1} = R_1$ dann auch (A2).
Für (A3) rechnen wir die Schnittzahlen explizit aus (es würde auch reichen zu argumentieren, dass sie konstant sind). Um die p_{ij}^0 zu berechnen seien zunächst $x, y \in X$ mit $(x, y) \in R_0$. Im Folgenden schreiben wir anstatt $(x, z) \in R_0$ kurz $x = z$ und anstelle von $(x, z) \in R_1$ kurz $x \neq z$, da dies jeweils äquivalent ist. Wir suchen nun:

- p_{00}^0 = Anzahl der $z \in X$ mit $x = z$ und $z = y$
- p_{01}^0 = Anzahl der $z \in X$ mit $x = z$ und $z \neq y$
- p_{10}^0 = Anzahl der $z \in X$ mit $x \neq z$ und $z = y$
- p_{11}^0 = Anzahl der $z \in X$ mit $x \neq z$ und $z \neq y$

Man sieht sofort, dass die Schnittzahlen nicht von der speziellen Wahl des Vertreters $(x, y) \in R_0$ abhängen, da es nur um Gleichheit oder Ungleichheit geht. Wegen $x = y$ erhalten wir sofort $p_{00}^0 = 1, p_{01}^0 = p_{10}^0 = 0$ und $p_{11}^0 = |X| - 1$.
Auf vollkommen analoge Weise berechnet man die Schnittzahlen p_{ij}^1. Dazu wählt man nun $x, y \in X$ mit $x \neq y$ beliebig (beachte $|X| \geq 2$) und zählt wieder dieselben Anzahlen wie zuvor (natürlich hängen die Anzahlen auch hier nicht von der speziellen Wahl von x und y ab). Mit $x \neq y$ erhalten wir $p_{00}^1 = 0, p_{10}^1 = p_{01}^1 = 1$ und $p_{11}^1 = |X| - 2$. Damit haben wir (A3) gezeigt und $(X, (R_0, R_1))$ ist ein (symmetrisches und kommutatives) Assoziationsschema mit einer Klasse.

1.2 Bemerkung. Ein Assoziationsschema (X, R) lässt sich als vollständiger, gerichteter Graph mit den Elementen von X als Ecken veranschaulichen, dessen Kanten mit den Zahlen von 0 bis n beschriftet sind. Zwei Ecken $x, y \in X$ sind genau dann durch eine mit i beschriftete Kante (kurz *i-Kante*) von x nach y verbunden, wenn $(x, y) \in R_i$ (also kann man im symmetrischen Fall auch einen ungerichteten Graphen betrachten). Dann ist v_i die Anzahl der von einem beliebigen Punkt $x \in X$ ausgehenden i-Kanten, ist also der (Außen-)Grad von x im Teilgraphen, der nur aus i-Kanten besteht. Die Valenz wird deshalb manchmal auch *Grad* genannt.
Axiom (A0) liefert die Vollständigkeit des Graphen und schließt Mehrfachkanten aus. Wegen Axiom (A1) ist jede Ecke durch eine mit 0 beschriftete Loop zu sich selbst verbunden, und nach Axiom (A2) ist das Umgekehrte einer i-Kante eine i^σ-Kante. Axiom (A3) sagt schließlich etwas über die Anzahl bestimmter Dreiecke aus: sind x und y durch eine (i.A. gerichtete) k-Kante verbunden, so ist die Anzahl der Dreiecke bestehend aus dieser Kante sowie einer i-Kante von x nach z und einer j-Kante von z nach y für

ein $z \in X$ gleich p_{ij}^k, unabhängig von der Wahl von x und y. Beweise können so auch kombinatorisch über das Abzählen in vollständigen Graphen geführt werden.

Wir formalisieren kurz die Bedeutung der Valenz, die auch schon in der Interpretation als Graph deutlich wurde:

1.3 Satz. *Sei (X, R) ein Assoziationsschema mit n Klassen. Für jedes $i \in \{0, \ldots, n\}$ gilt:*

$$v_i = |\{z \in X \mid (x, z) \in R_i\}|$$

für ein beliebiges $x \in X$.

Beweis. Sei (X, R) ein Assoziationsschema und $(x, x) \in R_0$ beliebig. Dann gilt:

$$\begin{aligned} v_i = p_{ii^\sigma}^0 &= |\{z \in X \mid (x, z) \in R_i \text{ und } (z, x) \in R_{i^\sigma}\}| \\ &= |\{z \in X \mid (x, z) \in R_i\}|, \end{aligned}$$

denn es gilt $(x, z) \in R_i \iff (z, x) \in R_{i^\sigma}$. □

Wie hilfreich die Interpretation eines Assoziationsschemas als Graph sein kann, zeigt der folgende Satz, in dem einige einfache Rechenregeln zusammengefasst sind.

1.4 Satz. *Sei (X, R) ein Assoziationsschema mit n Klassen. Dann gilt:*

(a) $\sum_{i=0}^{n} v_i = |X|$

(b) $p_{0j}^k = p_{j0}^k = \delta_{jk}$ *für alle* $j, k \in \{0, \ldots, n\}$

(c) $p_{ij}^k = p_{j^\sigma i^\sigma}^{k^\sigma}$ *für alle* $i, j, k \in \{0, \ldots, n\}$

Beweis. Zu (a): Nach (1.3) zählt v_i die von einem Punkt x ausgehenden i-Kanten. Wegen Axiom (A1) sind je zwei Punkte durch genau eine j-Kante und eine entgegengesetzte j^σ-Kante für ein $j \in \{0, \ldots, n\}$ verbunden (insbesondere gibt es auch eine Kante von x zu sich selbst). Die Summe über die Anzahlen der von einem Punkt x ausgehenden i-Kanten für $i = 0, \ldots, n$ ist also gleich der Anzahl *aller* von x ausgehenden Kanten, also gleich $|X|$.
Zu (b): Es sei $(x, y) \in R_k$. Dann gilt

$$\begin{aligned} p_{0j}^k &= |\{z \in X \mid (x, z) \in R_0 \text{ und } (z, y) \in R_j\}| \\ &= |\{z \in X \mid z = x \text{ und } (z, y) \in R_j\}| \\ &= |\{z \in X \mid z = x \text{ und } (x, y) \in R_j\}| = \delta_{jk}. \end{aligned}$$

Vollkommen analog beweist man $p_{j0}^k = \delta_{jk}$. Alternativ kann die Gleichheit auch wieder graphentheoretisch bewiesen werden: Seien $x, y \in X$ durch eine k-Kante von x nach y verbunden. Wir suchen nun die Anzahl der Dreiecke bestehend aus einer 0-Kante von x nach z und einer j-Kante von z nach y für $z \in X$. Da die 0-Kanten genau die Loops des Graphen sind, muss $z = x$ gelten, und da genau eine Kante von x nach y existiert, gibt

es so ein Dreieck offenbar genau dann, wenn $j = k$ gilt.
Zu (c): Wir zeigen, dass die Anzahlen der entsprechenden Dreiecke übereinstimmen. Für jedes Dreieck, das man für die Schnittzahl p_{ij}^k zählt, erhalten wir ein neues Dreieck, indem wir die drei beteiligten Kanten rückwärts laufen. Das so entstandene Dreieck ist dann eines der Dreiecke, die für die Schnittzahl $p_{j^\sigma i^\sigma}^{k^\sigma}$ gezählt werden müssen. Da die Zuordnung von Dreiecken für p_{ij}^k zu Dreiecken für $p_{j^\sigma i^\sigma}^{k^\sigma}$ nach den Axiomen (A0) und (A2) offenbar bijektiv ist, folgt die Behauptung. □

1.5 Korollar. *Jedes symmetrische Assoziationsschema ist kommutativ.*

Beweis. Ist (X, R) symmetrisch, so gilt $i^\sigma = i$ für alle $i = 0, \dots, n$. Mit (1.4c) folgt dann

$$p_{ij}^k = p_{j^\sigma i^\sigma}^{k^\sigma} = p_{ji}^k$$

für alle $i, j, k \in \{0, \dots, n\}$. □

Die Formulierung "symmetrisch und kommutativ" in Beispiel (1.1) war also überflüssig. Dies rechtfertigt außerdem, dass wir nur kommutative Assoziationsschemata betrachten, denn damit untersuchen wir auch alle symmetrischen.
Wir schauen uns nun das erste konkrete Schema an, nämlich das Hamming-Schema. Dieses Schema ist, wie wir in Kapitel 3 sehen werden, von besonderer Bedeutung in der Codierungstheorie.

1.6 Beispiel. Sei q eine Primzahlpotenz und $n \in \mathbb{N}$. Dann heißt $H(q, n) \coloneqq (\mathbb{F}_q^n, (R_i)_{i=0}^n)$ mit den Relationen

$$R_i \coloneqq \{(x, y) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \mid d(x, y) = i\},$$

das *Hamming-Schema* der Länge n über $\mathbb{F}_q$. Dabei bezeichnet $d(x, y)$ den Hammingabstand von x und y, also

$$d(x, y) = |\{i \in \{1, \dots, n\} \mid x_i \neq y_i\}|.$$

Offenbar bilden die R_i eine Partition von $\mathbb{F}_q^n \times \mathbb{F}_q^n$, also gilt (A0). Da d eine Metrik ist, sind außerdem (A1) und (A2) erfüllt. Insbesondere ist $H(q, n)$ symmetrisch. (A3) folgt aus der Translationsinvarianz des Hammingabstandes und der Tatsache, dass die Translation in $\mathbb{F}_q^n$ bijektiv ist, denn für $(x, y) \in R_k$ gilt

$$\begin{aligned} p_{ij}^k &= |\{z \in \mathbb{F}_q^n \mid d(x, z) = i,\ d(z, y) = j\}| \\ &= |\{z \in \mathbb{F}_q^n \mid d(0, z - x) = i,\ d(z - x, y - x) = j\}| \\ &= |\{\widetilde{z} \in \mathbb{F}_q^n \mid d(0, \widetilde{z}) = i,\ d(\widetilde{z}, \widetilde{y}) = j\}| \end{aligned}$$

für ein Element $\widetilde{y} \in \mathbb{F}_q^n$. Da die Grundmenge des Assoziationsschemas ganz $\mathbb{F}_q^n$ ist, sind mit $x, y, z \in \mathbb{F}_q^n$ auch $y - x, z - x$ Elemente von $\mathbb{F}_q^n$. Die Menge der $z \in \mathbb{F}_q^n$, die wir für p_{ij}^k bezüglich der Vertreter $(x, y) \in R_k$ zählen müssen, steht also über die Translation mit $-x$ in einer Bijektion zu der Menge der Elemente, die wir für p_{ij}^k bezüglich der Vertreter $(0, \widetilde{y})$ zählen müssen. Beachtet man, dass Permutationen und Skalierungen der

einzelnen Einträge keinen Einfluss auf den Hammingabstand haben, so kann man wegen des obigen Argumentes die Menge der $z \in \mathbb{F}_q^n$, die bezüglich x und y gezählt werden müssen, bijektiv auf die Menge der $z \in \mathbb{F}_q^n$ abbilden, die man zählen muss, wenn man x als 0 und y als das Wort mit k Einsen gefolgt von $n-k$ Nullen wählt. Da dies ein festes Paar von Worten ist, hängen die Schnittzahlen also nur von i, j und k ab, nicht aber von der Wahl der Vertreter x und y. Also gilt (A3) und damit ist $H(q,n)$ ein symmetrisches Assoziationsschema.

Wir berechnen nun die Valenzen von $H(q,n)$ und im Fall $q = 2$ auch die Schnittzahlen. Man beachte, dass (1.7) zwar für $q = 2$ ein Korollar aus (1.8) ist, (1.7) aber auch für beliebige Primzahlpotenzen ungleich 2 gilt.

1.7 Satz. *Für das Hamming-Schema $H(q,n)$ gilt*

$$v_i = \binom{n}{i}(q-1)^i$$

für alle $i \in \{0, \ldots, n\}$.

Beweis. Für ein festes $x \in \mathbb{F}_q^n$ ist v_i nach (1.3) die Anzahl der $z \in \mathbb{F}_q^n$, sodass $(x,z) \in R_i$ gilt. Also ist v_i die Anzahl der Vektoren $z \in \mathbb{F}_q^n$, die zu x den Hammingabstand i haben, sich also an genau i Stellen von x unterscheiden.
Sei nun $x \in \mathbb{F}_q^n$ beliebig. Es gibt $\binom{n}{i}$ mögliche Kombinationen der Stellen, an denen z sich von x unterscheiden kann. Für jede solche Möglichkeit gibt es pro Stelle genau $q-1$ Elemente aus $\mathbb{F}_q$, sodass sich z an dieser Stelle von x unterscheidet. Insgesamt gibt es also $v_i = \binom{n}{i}(q-1)^i$ solche z. □

1.8 Theorem. *Für die Schnittzahlen des binären Hamming-Schemas $H(2,n)$ gilt*

$$p_{ij}^k = \begin{cases} \binom{k}{\frac{i-j+k}{2}}\binom{n-k}{\frac{i+j-k}{2}} & , \text{falls } i-j+k \text{ gerade} \\ 0 & , \text{falls } i-j+k \text{ ungerade} \end{cases}$$

mit $\binom{n}{k} = 0$ für $k < 0$ oder $k > n$.

Beweis. Da die Schnittzahlen nach Axiom (A3) nur von i, j und k abhängen, können wir für die Berechnung ohne Beschränkung der Allgemeinheit ein Paar $(x,y) \in R_k$ mit $x = 0$ wählen. Dann ist y ein beliebiges Wort mit Hamminggewicht k. Gesucht ist nun die Anzahl der $z \in X$ mit $d(x,z) = d(0,z) = i$ (d.h. z muss Gewicht i haben) und $d(z,y) = j$.
Für einen Vektor z aus $\mathbb{F}_q^n$ bezeichne $r(z)$ die Anzahl der Einsen des Vektors, die mit den Einsen des gegebenen Vektors y übereinstimmen. Mit anderen Worten:

$$r(z) \coloneqq |\{m \in \{1, \ldots, n\} \mid z_m = y_m = 1\}|$$

Im Folgenden schreiben wir schlicht r anstelle von $r(z)$. Damit z Gewicht i hat, muss z noch $i - r$ weitere Einsen haben, und zwar an Stellen, an denen y eine 0 hat (sonst hätten wir den Eintrag bereits gezählt). Offenbar muss dann $r \in \{0, \dots, i\}$ gelten. Da wir zunächst aus den k Stellen, an denen y eine 1 hat, r Stellen auswählen, an denen z eine 1 hat, und anschließend auf die verbliebenen $n - k$ Stellen nochmal $i - r$ Einsen verteilen müssen, gibt es genau

$$a_r := \binom{k}{r}\binom{n-k}{i-r}$$

solche z. Ist dies nicht möglich (also zum Beispiel $r > k$ oder $r > i$), so ist a_r nach Definition des Binomialkoeffizienten gleich 0. Der Hammingabstand von y und einem solchen z ist

$$d(y, z) = (k - r) + (i - r) = k + i - 2r,$$

da y und z genau r Einsen gemeinsam haben (also tragen die restlichen $k - r$ Einsen von y zum Hammingabstand bei) und z noch $i - r$ weitere Einsen hat (und an diesen Stellen hat y Nullen). Damit z für p_{ij}^k gezählt wird, muss dieser Abstand nun gleich j sein. Umstellen nach r ergibt

$$d(y, z) = j \iff k + i - 2r = j \iff r = \frac{i - j + k}{2}.$$

Ein für gegebene i, j, k passendes r kann also genau dann gewählt werden, wenn $i - j + k$ gerade ist. In diesem Fall liefert a_r gerade die Anzahl der $z \in \mathbb{F}_q^n$ mit $d(x, z) = i$ und $d(z, y) = j$ für $(x, y) \in R_k$. Einsetzen von r liefert dann die Schnittzahl p_{ij}^k. Ist $i - j + k$ dagegen ungerade, so kann kein r gefunden werden, sodass $d(x, z) = i$ und $d(z, y) = j$ gilt, also ist in diesem Fall $p_{ij}^k = 0$. □

Man beachte, dass der Beweis in dieser Form nur für $q = 2$ gilt, da sonst aus $z_i \neq 0$ nicht $z_i = 1$ geschlossen werden kann. Dies wurde benötigt, um von der Anzahl der gemeinsamen Einsen direkt auf den Hammingabstand schließen zu können. Wir sehen, dass man die Valenz für beliebige n und q einfach berechnen konnte, die Schnittzahlen aber nur im Fall $q = 2$ leicht zu finden sind.

1.2 Die Bose-Mesner-Algebra

Dieser Abschnitt richtet sich nach Abschnitt 2.2 und 2.3 der Arbeit von Delsarte [4]. Einige Stellen sind der Arbeit "Association Schemes" von Godsil entnommen [6].
Wir wollen eine Möglichkeit finden, Assoziationsschemata mit algebraischen Methoden zu untersuchen. Dazu identifizieren wir die Relationen R_i mit ihren Adjazenzmatrizen A_i. Im Folgenden bezeichne $\mathbb{C}(X, X')$ für zwei nichtleere endliche Mengen X, X' die Menge aller $|X| \times |X'|$-Matrizen über $\mathbb{C}$, deren Zeilen mit X und deren Spalten mit X' indiziert sind. Für eine Matrix $A \in \mathbb{C}(X, X')$, $x \in X$ und $y \in X'$ bezeichnen wir den Eintrag in Zeile x und Spalte y von A mit $A(x, y)$.

Definition. Sei (X, R) ein Assoziationsschema. Für die Relation R_i heißt die quadratische Matrix $A_i \in \mathbb{C}(X, X)$ definiert durch

$$A_i(x, y) = \begin{cases} 1 \text{ , falls } (x, y) \in R_i \\ 0 \text{ , falls } (x, y) \notin R_i \end{cases}$$

die *Adjazenzmatrix* von R_i. Der von $A_0, \ldots, A_n$ erzeugte Untervektorraum $\mathcal{A}$ von $\mathbb{C}(X, X)$ heißt *Bose-Mesner-Algebra* des Assoziationsschemas.

Für die Adjazenzmatrizen gilt:

1.9 Satz. *Sei $\mathcal{A}$ die Bose-Mesner-Algebra eines Assoziationsschemas (X, R) mit n Klassen. Dann gilt für alle $i, j \in \{0, \ldots, n\}$:*

(a) $A_0 = I_{|X|}$

(b) $\sum_{k=0}^{n} A_k = J$, *wobei J die Matrix, deren Einträge alle 1 sind, bezeichnet.*

(c) $A_i^T \in \{A_0, \ldots, A_n\}$

(d) $A_i A_j = \sum_{k=0}^{n} p_{ij}^k A_k = A_j A_i$

Beweis. Zu (a): Klar nach Definition.
Zu (b): Wegen (A0) bilden die Relationen R_i eine Partition von $X \times X$. Für ein Paar $(x, y) \in X \times X$ tritt also in genau einer Adjazenzmatrix eine 1 an der Stelle (x, y) auf, in allen anderen steht dort eine 0. Die Summe aller A_i ist deshalb die Einsmatrix.
Zu (c): Offenbar ist A_i^T die Adjazenzmatrix der zu R_i inversen Relation R_i^{-1}. Wegen (A2) ist $R_i^{-1} \in \{R_0, \ldots, R_n\}$, also ist auch $A_i^T \in \{A_0, \ldots, A_n\}$.
Zu (d): Seien $i, j \in \{0, \ldots, n\}$. Wir halten zwei Elemente $x, y \in X$ fest und betrachten den Eintrag an der Stelle (x, y) im Produkt $A_i A_j$. Nach Definition der Matrixmultiplikation ist dieser gleich $\sum_{z \in X} A_i(x, z) A_j(z, y)$. Da die Adjazenzmatrizen nur aus Nullen und Einsen bestehen, ist ein Summand genau dann gleich 1, wenn $A_i(x, z) = A_j(z, y) = 1$, d.h. genau dann, wenn $(x, z) \in R_i$ und $(z, y) \in R_j$ gilt. Der Eintrag $A_i A_j(x, y)$ zählt also die Anzahl solcher z, denn in allen anderen Fällen ist der entsprechende Summand gleich 0. Nach (A3) ist diese Anzahl nur davon abhängig, in welcher Relation sich das Paar (x, y) befindet. Ist $(x, y) \in R_k$, so ist $A_i A_j(x, y) = p_{ij}^k$. Wegen $A_i(x, y) = \delta_{ik}$ ist in der Summe $\sum_{l=0}^{n} p_{ij}^l A_l$ für einen festen Eintrag immer nur höchstens ein Summand ungleich Null, und dieser ist gleich p_{ij}^k. Da x und y beliebig waren, stimmen die Matrizen $A_i A_j$ und $\sum_{k=0}^{n} p_{ij}^l A_l$ überein und vertauschen von i und j liefert $A_j A_i = \sum_{k=0}^{n} p_{ji}^k A_k$. Die Behauptung folgt nun sofort aus der Tatsache, dass wir nur kommutative Assoziationsschemata betrachten, d.h. es gilt $p_{ij}^k = p_{ji}^k$ für alle $i, j, k \in \{0, \ldots, n\}$, und damit haben wir

$$A_i A_j = \sum_{k=0}^{n} p_{ij}^k A_k = \sum_{k=0}^{n} p_{ji}^k A_k = A_j A_i.$$

□

Nach (d) ist $\mathcal{A}$ abgeschlossen bezüglich der Matrixmultiplikation. $\mathcal{A}$ ist also eine assoziative, kommutative Algebra (denn Matrixmultiplikation ist assoziativ und wegen (d) auch kommutativ in $\mathcal{A}$), und mit der Einheitsmatrix gibt es offenbar auch ein Neutralelement bezüglich der Multiplikation in $\mathcal{A}$. Aus (b) folgt, dass die A_i linear unabhängig sind, denn ist eine Linearkombination der A_i gleich der Nullmatrix, so müssen alle Skalare schon 0 gewesen sein, denn für eine feste Stelle (x, y) hat immer nur genau eine der Adjazenzmatrizen einen Eintrag ungleich 0. Die Dimension von $\mathcal{A} = span(A_0, \ldots, A_n)$ ist deshalb gerade $n + 1$. Insbesondere bilden die A_i eine Basis von $\mathcal{A}$.
Wir zeigen nun, dass man die Eigenschaften aus (1.9) auch als Definition für Assoziationsschemata verwenden kann, diese also äquivalent zu den Axiomen (A0) bis (A3) sind. Dann können wir ein Assoziationsschema auch durch Betrachtung der zugehörigen Bose-Mesner-Algebra untersuchen.

1.10 Satz. *Sei X eine nichtleere endliche Menge mit $|X| \geq 2$ und $\{A_0, \ldots, A_n\} \subseteq \mathbb{C}(X, X)$, $n \in \mathbb{N}$, eine Menge von $n + 1$ Matrizen mit Einträgen in $\{0, 1\}$, die die Eigenschaften (a) bis (d) aus (1.9) hat, und sei $\mathcal{A}$ der von $A_0, \ldots, A_n$ erzeugte Untervektorraum von $\mathbb{C}(X, X)$. Dann ist $\mathcal{A}$ die Bose-Mesner-Algebra eines Assoziationsschemas (X, R) mit n Klassen. Dabei ist das Assoziationsschema eindeutig durch X und $\mathcal{A}$ bestimmt.*

Beweis. Definiere auf $X \times X$ die binären Relationen R_i durch

$$(x, y) \in R_i :\Leftrightarrow A_i(x, y) = 1 \quad (\text{beachte } A_i(x, y) \in \{0, 1\}).$$

Offenbar sind die Relationen eindeutig durch die Matrizen bestimmt. Wegen $A_0 = I_n$ gilt dann $R_0 = \{(x, x) \in X \times X \mid x \in X\}$ und wegen $\sum_{i=0}^{n} A_i = J$ bilden die R_i eine Partition von $X \times X$ (beachte, dass alle Einträge der Matrizen A_i entweder 0 oder 1 sind), also gelten (A0) und (A1), und die A_i sind genau die Adjazenzmatrizen der zugehörigen Relationen. Da A_i^T die Adjazenzmatrix der zu R_i inversen Relation R_i^{-1} ist, gilt wegen $A_i^T \in \{A_0, \ldots, A_n\}$ auch $R_i^{-1} \in \{R_0, \ldots, R_n\}$, also gilt (A2).
Zu (A3): Zu zeigen ist, dass für $(x, y) \in R_k$ die Anzahl der $z \in X$ mit $(x, z) \in R_i$ und $(z, y) \in R_j$ nur von i, j, k abhängt. Betrachtet man das Produkt $A_i A_j$, so steht an der Stelle (x, y) (wie wir im Beweis von (1.9d) gesehen haben) genau die Anzahl der $z \in X$ mit $(x, z) \in R_i$ und $(z, y) \in R_j$. Für $(x, y) \in R_k$ ist diese Anzahl nach (1.9d) also

$$A_i A_j(x, y) = \left(\sum_{l=0}^{n} p_{ij}^l A_l \right)(x, y) = \sum_{l=0}^{n} \left(p_{ij}^l A_l(x, y) \right) = \sum_{l=0}^{n} p_{ij}^l \delta_{kl} = p_{ij}^k.$$

Außerdem erhalten wir aus (1.9d) auch sofort $p_{ij}^k = p_{ji}^k$ für alle $i, j, k \in \{0, \ldots, n\}$. Die Schnittzahlen sind also konstant und $(X, (R_i)_{i=0}^n)$ ist ein Assoziationsschema. □

Um die Bose-Mesner-Algebra (und damit Assoziationsschemata) genauer untersuchen zu können, benötigen wir folgende bekannte Eigenschaft von quadratischen, normalen Matrizen:

1.11 Satz. *Sei $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ eine nichtleere Menge normaler, kommutierender Matrizen, d.h. $A\,\overline{A}^T = \overline{A}^T A$ und $AB = BA$ für alle $A, B \in \mathcal{A}$. Dann gibt es eine unitäre Matrix $S \in \mathbb{C}^{n\times n}$, sodass $S^{-1}\mathcal{A}S = \{S^{-1}AS \mid A \in \mathcal{A}\}$ nur aus Diagonalmatrizen besteht.*

Für einen Beweis siehe etwa Theorem 2 in [11].

Wir konstruieren nun eine weitere Basis von $\mathcal{A}$, die aus idempotenten und paarweise orthogonalen Matrizen besteht. Dazu definieren wir:

Definition. Sei X eine endliche nichtleere Menge und $\pi = \{X_k \subseteq X \mid k = 0, \ldots, n\}$ eine Partition der Menge X in $n+1$ nichtleere Teilmengen. Zu dieser Partition definieren wir die $n+1$ Diagonalmatrizen $\Gamma_k \in \mathbb{C}(X, X)$, $k = 0, \ldots, n$, durch

$$\Gamma_k(x,x) = \begin{cases} 1 & , \text{ falls } x \in X_k \\ 0 & , \text{ sonst} \end{cases}$$

und $\Gamma_k(x, y) = 0$ für $x \neq y$.

Definition. Für eine unitäre Matrix $S \in \mathbb{C}(X, X)$ und eine Partition $\pi = \{X_k \subseteq X \mid k = 0, \ldots, n\}$ von X definieren wir

$$E_k = S\,\Gamma_k\,\overline{S}^T = S_k\,\overline{S_k}^T$$

für $k = 0, \ldots, n$, wobei S_k die $|X| \times |X_k|$-Matrix ist, die genau die zu X_k gehörenden Spalten enthält.

1.12 Theorem. [4, Theorem 2.2] *Sei (X, R) ein Assoziationsschema mit n Klassen. Dann gibt es eine Partition π von X in $n+1$ Mengen X_k, $k = 0, \ldots, n$, mit $|X_0| = 1$ und eine unitäre Matrix $S \in \mathbb{C}(X, X)$, sodass die Matrizen $E_0, \ldots, E_n$ eine Basis der Bose-Mesner-Algebra $\mathcal{A}$ des Assoziationsschemas bilden. Dabei kann ohne Beschränkung der Allgemeinheit*

$$S_0 = \frac{1}{\sqrt{|X|}}(1, \ldots, 1)^T$$

als erste Spalte der Matrix S gewählt werden (die zu X_0 gehörende Spalte).

Beweis. Da $\mathcal{A}$ kommutativ ist und mit A auch $\overline{A}^T$ in $\mathcal{A}$ liegt (nach Satz (1.9)), ist jede Matrix aus $\mathcal{A}$ normal. Also gibt es nach Satz (1.11) eine unitäre Matrix $S \in \mathbb{C}(X, X)$, sodass $\widetilde{\mathcal{A}} \coloneqq S^{-1}\mathcal{A}S = \{S^{-1}AS \mid A \in \mathcal{A}\}$ nur aus Diagonalmatrizen besteht. Dabei sind die Einträge auf der Diagonalen einer Matrix in $\widetilde{\mathcal{A}}$ gerade ihre Eigenwerte. Man beachte, dass $\widetilde{\mathcal{A}}$ eine zu $\mathcal{A}$ isomorphe Algebra ist (denn die Konjugation mit S ist ein Isomorphismus von $\mathcal{A}$ auf $\widetilde{\mathcal{A}}$).
Sei nun M eine Matrix in $\mathcal{A}$, die maximal viele verschiedene Eigenwerte hat. Diese Anzahl sei $n' + 1$, und die Eigenwerte seien $\lambda_0, \ldots, \lambda_{n'}$. Dann gibt es eine Partition π von X in $n' + 1$ Klassen $X_k, k = 0, \ldots, n'$, sodass wir schreiben können

$$\Lambda \coloneqq S^{-1}MS = \sum_{k=0}^{n'} \lambda_k \Gamma_k.$$

Dazu wählen wir X_k als Menge der Spaltenindizes von Λ, in denen der Eigenwert λ_k steht. Da die λ_k verschieden und endlich viele sind, können wir Polynome $f_i(x)$ über $\mathbb{C}$ finden, sodass $f_i(\lambda_k) = \delta_{ik}$ für alle $i, k = 0, \ldots, n'$ gilt (dies folgt sofort aus einem wohlbekannten Interpolationsresultat, wie es beispielsweise in der Numerik gelehrt wird: Zu $n+1$ gegebenen verschiedenen Zahlen $x_0, \ldots, x_n \in \mathbb{C}$ und beliebigen $y_0, \ldots, y_n \in \mathbb{C}$ kann man immer ein Polynom über $\mathbb{C}$ vom Grad n finden, sodass $f(x_i) = y_i$ für alle $i = 0, \ldots, n$). Setzen wir nun Λ in diese Polynome ein (indem wir $\Lambda^0 = I_{|X|}$ setzen), erhalten wir $f_k(\Lambda) = f_k(\sum_{i=0}^{n'} \lambda_i \Gamma_i) = \Gamma_k$, da nach Definition der Matrizen Γ_k für alle $i, j = 0, \ldots, n$ gilt:

$$\Gamma_i \Gamma_j = \delta_{ij} \Gamma_i.$$

Gemischte Terme fallen also weg und da die Γ_k Diagonalmatrizen sind, ist $f_k(\Lambda)$ eine Diagonalmatrix mit Einträgen $f_k(\lambda_j) = \delta_{kj}$ auf der Diagonalen, wobei λ_j der Eigenwert ist, der an entsprechender Position in Λ steht. Nach Definition der f_i erhalten wir somit das Gewünschte. Daraus folgt, dass die Γ_k zur Algebra $\widetilde{\mathcal{A}}$ gehören, da sie als Linearkombination von Potenzen der Matrix $\Lambda \in \widetilde{\mathcal{A}}$ geschrieben werden können.
Umgekehrt erzeugen die Matrizen Γ_k bereits die ganze Algebra $\widetilde{\mathcal{A}}$. Denn gäbe es eine Matrix $A \in \mathcal{A}$, die sich nicht als Linearkombination der Γ_k darstellen lässt, so müsste es ein $i \in \{0, \ldots, n'\}$ geben, sodass die Einträge in den zu X_i gehörenden Spalten von A nicht alle gleich sind. Dann ist auch $\Gamma_i A$ ein Element von $\widetilde{\mathcal{A}}$ (und zwar eine Matrix, die nur Einträge auf der Diagonalen in den zu X_i gehörigen Spalten hat, welche nicht alle gleich sind), und wir könnten aus den Matrizen Γ_k und $\Gamma_i A$ eine Matrix als Linearkombination konstruieren, die mehr als $n'+1$ verschiedene Eigenwerte hat, beispielsweise $A' \coloneqq \sum_{k=0}^{n'} k\Gamma_k + \lambda \Gamma_i A$. Dann hätte A' bereits n' verschiedene Eigenwerte (nämlich $0, \ldots, n'$ außer i von den Matrizen $0 \cdot \Gamma_0, \ldots, (i-1) \cdot \Gamma_{i-1}, (i+1) \cdot \Gamma_{i+1}, \ldots, n' \cdot \Gamma_{n'}$) und durch passende Wahl von λ kämen mindestens zwei neue hinzu. Dies ist aber ein Widerspruch dazu, dass $n'+1$ die maximale Anzahl an Eigenwerten einer Matrix aus $\widetilde{\mathcal{A}}$ ist, und damit erzeugen die Γ_k die Algebra $\widetilde{\mathcal{A}}$. Somit gilt $n = n'$.
Da die Γ_k nun genau dimensionsviele linear unabhängige Matrizen sind, bilden sie eine Basis aus idempotenten Elementen von $\widetilde{\mathcal{A}}$. Also sind die E_k eine Basis von $\mathcal{A}$, da sie genau die Urbilder der Γ_k unter der Konjugation mit S sind (denn es ist $S^{-1} = \overline{S}^T$).
Schließlich beobachten wir, dass die Einsmatrix J als Summe aller Adjazenzmatrizen ein Element von $\mathcal{A}$ ist. Da diese offenbar genau einmal den Eigenwert $|X|$ hat (zum Beispiel mit Eigenvektor $(1, \ldots, 1)^T$) und $|X|-1$ mal den Eigenwert 0 (da ihr Rang gleich 1 ist), muss eine der Teilmengen X_k der Partition π genau ein Element enthalten, weil sich die Matrix $SJS^{-1} = diag(|X|, 0 \ldots, 0)$ als Linearkombination der Γ_k schreiben lässt. Ohne Beschränkung der Allgemeinheit sei dies die Teilmenge X_0 (sonst Umnummerierung der Teilmengen). Als zu X_0 gehörige Spalte steht in S dann der Vektor

$$\alpha \cdot \frac{1}{\sqrt{|X|}} (1, \ldots, 1)^T$$

für ein $\alpha \in \mathbb{C}$ mit $\alpha\overline{\alpha} = 1$ (denn S ist unitär). Da mit S auch die mit $\overline{\alpha}$ skalierte Matrix $\overline{\alpha}S$ unitär ist, können wir ohne Einschränkung annehmen, dass $\alpha = 1$ ist, und das Theorem ist bewiesen. □

Im Folgenden werden wir aufgrund von Theorem (1.12) immer mit den zwei Basen $A_0, \ldots, A_n$ und $E_0, \ldots, E_n$ rechnen, ohne eine Partition und eine unitäre Matrix anzugeben, da diese für die weitere Untersuchung nicht relevant sind. Es reicht aus zu wissen, dass die Basis existiert und welche Rechenregeln sie erfüllt (siehe (1.15)). Der Beweis von (1.12) zeigt nämlich auch, dass die Partition π (und damit die Matrizen E_k) bis auf Nummerierung der Teilmengen eindeutig bestimmt ist, da sich *jede* Matrix aus der diagonalisierten Algebra $\widetilde{\mathcal{A}}$ als Linearkombination der Γ_k schreiben lässt. Es ist also egal, welche Matrix mit maximal vielen verschiedenen Eigenwerten man für die Konstruktion der Partition π nimmt. Des Weiteren setzen wir $E_0 \coloneqq \frac{1}{|X|}J$, da dies die zu Γ_0 gehörige Basismatrix von $\mathcal{A}$ ist.

1.13 Bemerkung. Die Matrizen E_k entsprechen den maximalen gemeinsamen Eigenräumen, d.h. den Untervektorräumen von $\mathbb{F}_q^n$, dessen Elemente ungleich 0 für jede Matrix in $\mathcal{A}$ Eigenvektoren zum selben Eigenwert sind, und die maximal bezüglich dieser Eigenschaft sind:
Wir betrachten die Spalten von S, die zu einer festen Matrix Γ_k gehören. Diese sind Eigenvektoren zum selben Eigenwert für *jede* Matrix in $\mathcal{A}$, da S die Bose-Mesner-Algebra diagonalisiert. Dabei können sich die zugehörigen Eigenwerte von Matrix zu Matrix unterscheiden, aber für jede Matrix in $\mathcal{A}$ gehören die betrachteten Spalten von S zum selben Eigenwert. Der Spann dieser Spalten ist nach Definition der Γ_k über eine Matrix mit maximal vielen verschiedenen Eigenwerten folglich gleich einem der maximalen gemeinsamen Eigenräume.
Etwas anders betrachtet kann man die E_k auch als minimal bezeichnen und sie werden deshalb auch Basis der minimalen Idempotente genannt. Denn ihre Spalten sind (wie die Spalten von S) Eigenvektoren für jede Matrix aus $\mathcal{A}$ und zusammengenommen erzeugen die Spalten aller E_k ganz $\mathbb{C}^{|X|}$. Dabei besteht eine Matrix E_k aber komplett aus Eigenvektoren aus *einem* der maximalen gemeinsamen Eigenräume, und nicht aus mehreren. Da wir wollen, dass die Spalten einer Matrix E_k eine Basis eines maximalen gemeinsamen Eigenraumes enthalten, sind die E_k in diesem Sinne minimal.
Die Minimalität der E_k wird deutlicher, wenn man sie wie Godsil in Abschnitt 1.4 in [6] definiert: Dort werden Assoziationsschemata über die Adjazenzmatrizen und die Bose-Mesner-Algebra eingeführt und die Matrizen E_k werden ein wenig anders konstruiert. Wir definieren dazu auf den Idempotenten von $\mathcal{A}$ die Relation

$$E \leq F :\Longleftrightarrow FE = E$$

für alle idempotenten $E, F \in \mathcal{A}$. Man sieht leicht, dass diese Relation reflexiv, antisymmetrisch und transitiv ist, $\leq$ ist also eine Halbordnung. Die minimalen idempotenten Elemente ungleich der Nullmatrix bilden dann eine Basis von $\mathcal{A}$. Da wir aber Assoziationsschemata über Relationen und nicht wie in [6] über Matrizen und die von ihnen erzeugte Algebra definiert haben, ist die Konstruktion der E_k wie in Theorem (1.12) einfacher als über die Relation $\leq$. Offensichtlich sind die Matrizen Γ_k (und damit auch die Matrizen E_k) minimale Idempotente bezüglich der Halbordnung $\leq$.

1.14 Bemerkung. Wie wir im Beweis von (1.12) gesehen haben, lassen sich alle Matrizen der Bose-Mesner-Algebra $\mathcal{A}$ eines Assoziationsschemas simultan diagonalisieren.

Ist (X, R) dabei ein symmetrisches Assoziationsschema, so lässt sich die Bose-Mesner-Algebra auch über $\mathbb{R}$ betrachten, denn da alle Relationen symmetrisch sind, sind auch die Adjazenzmatrizen A_i der Relationen symmetrisch. Damit sind auch beliebige Linearkombinationen der A_i symmetrisch, und da sie paarweise kommutieren (siehe (1.9)) sogar beliebige Produkte der A_i. Also sind alle Matrizen in $\mathcal{A}$ symmetrisch und haben damit nur reelle Eigenwerte. Die Diagonalisierung kann deshalb auch über $\mathbb{R}$ erfolgen.

Im Folgenden benötigen wir einige einfache Eigenschaften der Basis aus minimalen idempotenten Matrizen:

1.15 Satz. [6, Theorem 1.5.1] *Die Basis $E_0, \ldots, E_n$ der Bose-Mesner-Algebra aus minimalen Idempotenten erfüllt:*

(a) $E_i E_j = 0$ *für alle* $i \neq j$

(b) $\sum_{k=0}^{n} E_k = I$

(c) $\overline{E_k}^T = E_k$ *für alle* $k = 0, \ldots, n$*, die* E_k *sind also hermitesche Matrizen.*

Beweis. Zu (a): Seien $i, j \in \{0, \ldots, n\}, i \neq j$. Dann gilt:

$$E_i E_j = (S\,\Gamma_i\,\overline{S}^T)(S\,\Gamma_j\,\overline{S}^T) = (S\,\Gamma_i\Gamma_j\,\overline{S}^T) = 0,$$

da $\Gamma_i\Gamma_j = 0$ für $i \neq j$.
Zu (b): Es gilt

$$\sum_{k=0}^{n} E_k = \sum_{k=0}^{n}(S\,\Gamma_k\,\overline{S}^T) = S(\sum_{k=0}^{n}\Gamma_k)\overline{S}^T = SI\overline{S}^T = I$$

nach Definition der Γ_k und weil S unitär ist.
Zu (c): Die E_k sind hermitesch, denn es gilt für jedes $k = 0, \ldots, n$

$$\overline{E_k}^T = \left(\overline{S\,\Gamma_k\,\overline{S}^T}\right)^T = S\,\overline{\Gamma_k}^T\,\overline{S}^T = S\,\Gamma_k\,\overline{S}^T = E_k,$$

da die Γ_k Diagonalmatrizen mit Einträgen 0 und 1 auf der Diagonalen sind. □

Wir definieren nun noch eine weitere Größe, die bei der Untersuchung von Assoziationsschemata eine Rolle spielt.

Definition. Seien (X, R) ein Assoziationsschema mit n Klassen, A_i die Adjanzenzmatrix der Relation R_i für $i = 0, \ldots, n$, und $\mathcal{A}$ die Bose-Mesner-Algebra des Assoziationsschemas. Weiter sei $E_0, \ldots E_n$ die Basis aus minimalen, idempotenten Matrizen. Dann lassen sich die beiden Basen in der jeweils anderen darstellen als

$$A_i = \sum_{k=0}^{n} p_i(k)E_k \quad \text{und} \quad E_k = \frac{1}{|X|}\sum_{i=0}^{n} q_k(i)A_i$$

für Skalare $p_i(k) \in \mathbb{C}$, genannt *Eigenwerte* des Schemas, und $q_i(k) \in \mathbb{C}$, genannt *duale Eigenwerte* des Schemas $(i, k \in \{0, \ldots, n\})$.

1.16 Bemerkung. Wegen $A_0 = I$ und der Eindeutigkeit der Basisdarstellung gilt nach (1.15b)

$$p_0(k) = 1 \text{ für alle } k = 0, \ldots, n,$$

und aufgrund von (1.9b) gilt analog

$$q_0(i) = 1 \text{ für alle } i = 0, \ldots, n.$$

Da außerdem $E_i E_j = 0$ für $i \neq j$ gilt, folgt

$$A_i E_k = \left(\sum_{l=0}^{n} p_i(l) E_l \right) E_k = p_i(k) E_k, \qquad (*)$$

da die E_k idempotent sind. Die Eigenwerte des Assoziationsschemas sind also genau die Eigenwerte der Adjazenzmatrizen, da die Spalten der E_k Eigenvektoren jeder Adjazenzmatrix sind. Die A_i können außerdem keine weiteren Eigenwerte haben, da die Spalten der E_k zusammmen genommen schon ganz $\mathbb{C}^{|X|}$ erzeugen und damit eine Basis von $\mathbb{C}^{|X|}$ enthalten.
Insbesondere haben wir

$$A_i J = v_i J$$

und mit $E_0 = \frac{1}{|X|} J$ und $(*)$ folgt

$$v_i E_0 = A_i E_0 = p_i(0) E_0,$$

also $p_i(0) = v_i$ für $i = 0, \ldots, n$. Analog können wir $q_k(0)$ durch Betrachtung der Spur (Notation: tr) berechnen:

$$tr(E_k) = \frac{1}{|X|} \sum_{i=0}^{n} q_k(i) tr(A_i)$$

und da $tr(A_i) = 0$ für $i \neq 0$ sowie $tr(A_0) = |X|$ gelten, folgt

$$Rang(E_k) = tr(E_k) = \frac{1}{|X|} q_k(0) |X| = q_k(0)$$

für $k = 0, \ldots, n$. Da die Eigenwerte eines Schemas offenbar gerade den Einträgen der Basiswechselmatrix entsprechen, erhält man die jeweils anderen Eigenwerte durch Invertieren der entsprechenden Matrix. Genauer: Definiert man die Matrizen $P := (p_{ij})$ mit $p_{ij} := p_j(i)$ und $Q := (q_{ij})$ mit $q_{ij} := q_j(i)$ $(i, j = 0, \ldots, n)$, so lässt sich diese Eigenschaft schreiben als

$$PQ = |X| I_{n+1}.$$

1.17 Bemerkung. [6, Abschnitt 2.3] Die Schnittzahlen p_{ij}^k und die Eigenwerte $p_i(k)$ (und damit auch die dualen Eigenwerte $q_k(i)$) hängen voneinander ab. Es gilt nämlich für alle $i, j, k\{0, \ldots, n\}$:

$$tr(A_i A_j A_k^T) = tr((\sum_{l=0}^{n} p_{ij}^l A_l) A_k^T) = tr(p_{ij}^k A_k A_k^T) = p_{ij}^k v_k |X|,$$

denn die Diagonale der Matrizen $A_l A_k^T$ besteht jeweils aus den Skalarprodukten derselben Zeilen von A_l und A_k. Diese sind für $k \neq l$ alle gleich 0, denn wäre ein Eintrag im Produkt $A_l A_k^T$ ungleich 0, so gäbe es $x, y \in X$ mit $(x, y) \in R_l$ und $(x, y) \in R_k$. Ein Eintrag auf der Diagonalen in $A_l A_k^T$ kann nämlich nur dann ungleich 0 sein, wenn es eine Stelle gibt, an der A_l und A_k beide eine 1 haben. Da die Relationen R_i aber $X \times X$ partitionieren, kann dieser Fall nicht auftreten. Analog erhält man die Diagonaleinträge von $A_k A_k^T$, denn hier zählen die Skalarprodukte einer Zeile mit sich selbst die Anzahl der Einsen dieser Zeile. Diese Anzahl ist nach (1.3) aber konstant und gerade v_k. Also ist jeder Eintrag auf der Diagonalen von $A_i A_j A_k^T$ gleich $p_{ij}^k v_k$ und die Spur ist somit gleich $p_{ij}^k v_k |X|$.
Andererseits wissen wir aus der linearen Algebra, dass die Spur von $A_i A_j A_k^T$ die Summe ihrer Eigenwerte ist. Außerdem wissen wir nach (1.16), dass für jedes $i = 0, \ldots, n$ die Zahlen $p_i(k), k = 0, \ldots, n$, schon alle Eigenwerte von A_i sind.
Da alle Matrizen in $\mathcal{A}$ simultan diagonalisierbar sind, haben sie alle dieselben Eigenvektoren, und damit sind die Eigenwerte des Produktes zweier Matrizen die Produkte der Eigenwerte zu denselben Eigenvektoren. Außerdem sind die Eigenwerte einer Matrix A (über $\mathbb{C}$) gleich den Konjugierten der Eigenwerte von A^T. Da $tr(E_k) = Rang(E_k)$ für jedes i die Vielfachheit des Eigenwerts $p_i(k)$ ist, erhalten wir

$$p_{ij}^k v_k |X| = tr(A_i A_j A_k^T) = \sum_{l=0}^{n} tr(E_l) p_i(l) p_j(l) \overline{p_k(l)},$$

und schließlich

$$p_{ij}^k = \frac{1}{|X| v_k} \sum_{l=0}^{n} tr(E_l) p_i(l) p_j(l) \overline{p_k(l)}.$$

Die Schnittzahlen sind also nicht unabhängig von den Eigenwerten. Allerdings benutzt man diese Formel in der Regel nicht zum Berechnen der Schnittzahlen, da das Berechnen der Eigenwerte oft schwieriger ist als das Berechnen der Schnittzahlen.

Um die bisher definierten Begriffe zu verdeutlichen, untersuchen wir im folgenden Beispiel die Bose-Mesner-Algebra von $H(2, 3)$:

1.18 Beispiel. Wir betrachten $H(2, 3)$, also das binäre Hamming-Schema der Länge 3. Die Bose-Mesner-Algebra besteht hier aus (8×8)-Matrizen. Wir sortieren die Elemente aus $\mathbb{F}_2^3$ in der Reihenfolge 000,001,010,100,011,101,110,111. Dadurch erreichen wir, dass die Adjazenzmatrizen symmetrisch bezüglich der Gegendiagonalen sind. Symmetrisch bezüglich der Hauptdiagonalen sind sie immer, da $H(2, 3)$ ein symmetrisches Assoziationsschema ist. Wir können die Adjazenzmatrizen direkt hinschreiben, denn nach Definition ist der Eintrag $A_i(x, y)$ genau dann gleich 1, wenn x und y Hammingabstand i

haben. Das liefert die Adjazenzmatrizen

$$A_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \; A_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \; A_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Da für alle $x, y \in \mathbb{F}_2^3$ der Eintrag $A_i(x, y)$ für genau ein $i \in \{0, 1, 2, 3\}$ ungleich 0 ist, kann man das Produkt zweier Matrizen leicht als Linearkombination der A_i schreiben. Wir erhalten

$$\begin{aligned} A_1A_1 &= 3A_0 + 2A_2 \\ A_1A_2 &= 2A_1 + 3A_3 \\ A_1A_3 &= A_2 \\ A_2A_2 &= 3A_0 + 2A_2 \\ A_2A_3 &= A_1 \\ A_3A_3 &= A_0 \end{aligned}$$

und lesen nun zeilenweise als Skalare in den Linearkombinationen die Schnittzahlen ab. Da $H(2, 3)$ (und damit die Matrixmultiplikation in der Bose-Mesner-Algebra von $H(2, 3)$) kommutativ ist, geben wir nur die Schnittzahlen p_{ij}^k mit $i \leq j$ an:

$$\begin{array}{llll} p_{11}^0 = 3, & p_{11}^1 = 0, & p_{11}^2 = 2, & p_{11}^3 = 0 \\ p_{12}^0 = 0, & p_{12}^1 = 2, & p_{12}^2 = 0, & p_{12}^3 = 3 \\ p_{13}^0 = 0, & p_{13}^1 = 0, & p_{13}^2 = 1, & p_{13}^3 = 0 \\ p_{22}^0 = 3, & p_{22}^1 = 0, & p_{22}^2 = 2, & p_{22}^3 = 0 \\ p_{23}^0 = 0, & p_{23}^1 = 1, & p_{23}^2 = 0, & p_{23}^3 = 0 \\ p_{33}^0 = 1, & p_{33}^1 = 0, & p_{33}^2 = 0, & p_{33}^3 = 0 \end{array}$$

Wir berechnen nun die Basis aus idempotenten Matrizen. Man kann die Einträge der Matrizen E_k für beliebige q und n explizit ausrechnen (siehe Theorem 5 in Kapitel 21 in [10]). Hier wollen wir aber noch einmal die Konstruktion aus Theorem (1.12) illustrieren. Mithilfe eines Computers lässt sich leicht überprüfen, dass die Matrix A_1 vier verschiedene Eigenwerte, nämlich $-3, -1, 1$ und 3, hat. Da die Bose-Mesner-Algebra von $H(2,3)$ Dimension 4 hat sind dies maximal viele. Wie aus der linearen Algebra bekannt, können wir nun Basen der Eigenräume bestimmen und diese mit dem Gram-Schmidt-Verfahren zu einer Orthonormalbasis aus Eigenvektoren zusammensetzen. Wir erhalten etwa

$$\widetilde{S} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 & 1 & 1 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 1 & -1 & 0 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}$$

als Transformationsmatrix, welche die Diagonalgestalt

$$\widetilde{S}^{-1} A_1 \widetilde{S} = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -3 \end{pmatrix}$$

liefert. Nun wenden wir das Gram-Schmidt-Verfahren jeweils auf die Spalten 2 bis 4 und 5 bis 7 von $\widetilde{S}$ an, um eine unitäre Matrix S zu erhalten. Da S Wurzeln und Brüche enthält, geben wir es der Übersichtlichkeit halber hier nicht an. Wir bezeichnen nun mit S_1 die erste Spalte von S, mit S_{234} die Spalten 2 bis 4, mit S_{567} die Spalten 5 bis 7 und mit S_8 die letzte Spalte von S. Als idempotente Basismatrizen erhalten wir dann nach Theorem (1.12)

$$E_0 = S_1 S_1^T = \frac{1}{8} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Dies ist immer die erste idempotente Basismatrix und hätte nicht explizit berechnet werden müssen. Die anderen Basismatrizen berechnen sich zu

$$E_1 = S_{234}S_{234}^T = \frac{1}{8}\begin{pmatrix} 3 & 1 & 1 & 1 & -1 & -1 & -1 & -3 \\ 1 & 3 & -1 & -1 & 1 & 1 & -3 & -1 \\ 1 & -1 & 3 & -1 & 1 & -3 & 1 & -1 \\ 1 & -1 & -1 & 3 & -3 & 1 & 1 & -1 \\ -1 & 1 & 1 & -3 & 3 & -1 & -1 & 1 \\ -1 & 1 & -3 & 1 & -1 & 3 & -1 & 1 \\ -1 & -3 & 1 & 1 & -1 & -1 & 3 & 1 \\ -3 & -1 & -1 & -1 & 1 & 1 & 1 & 3 \end{pmatrix},$$

$$E_2 = S_{567}S_{567}^T = \frac{1}{8}\begin{pmatrix} 3 & -1 & -1 & -1 & -1 & -1 & -1 & 3 \\ -1 & 3 & -1 & -1 & -1 & -1 & 3 & -1 \\ -1 & -1 & 3 & -1 & -1 & 3 & -1 & -1 \\ -1 & -1 & -1 & 3 & 3 & -1 & -1 & -1 \\ -1 & -1 & -1 & 3 & 3 & -1 & -1 & -1 \\ -1 & -1 & 3 & -1 & -1 & 3 & -1 & -1 \\ -1 & 3 & -1 & -1 & -1 & -1 & 3 & -1 \\ 3 & -1 & -1 & -1 & -1 & -1 & -1 & 3 \end{pmatrix},$$

$$E_3 = S_8S_8^T = \frac{1}{8}\begin{pmatrix} 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \end{pmatrix}.$$

Für jedes $i, k \in \{0, 1, 2, 3\}$ können wir nun das Produkt A_iE_k ausrechnen. So erhalten wir leicht die Koeffizienten, um die A_i als Linearkombination der E_k zu schreiben (siehe (1.16)). Beispielsweise gilt

$$A_2E_0 = 3E_0, \quad A_2E_1 = -E_1, \quad A_2E_2 = -E_2, \quad A_2E_3 = 3E_3$$

und wir können schreiben

$$A_2 = 3E_0 - E_1 - E_2 + 3E_3.$$

Insgesamt erhält man

$$\begin{aligned} A_0 &= E_0 + E_1 + E_2 + E_3, \\ A_1 &= 3E_0 + E_1 - E_2 - 3E_3, \\ A_2 &= 3E_0 - E_1 - E_2 + 3E_3, \\ A_3 &= E_0 - E_1 + E_2 - E_3. \end{aligned}$$

Schreiben wir die Koeffizienten spaltenweise in eine Matrix, so erhalten wir die Basiswechselmatrix von der Basis der A_i zur Basis der E_k. Diese ist gegeben durch

$$P = \begin{pmatrix} 1 & 3 & 3 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -3 & 3 & -1 \end{pmatrix}.$$

Dabei gilt $P(k,i) = p_i(k)$. Die dualen Eigenwerte erhalten wir nun einfach durch Invertieren und Skalieren der Matrix P, siehe (1.16). Dann ist $q_k(i)$ der Eintrag an der Stelle (k,i) der Matrix

$$Q = |X|P^{-1} = P,$$

also $p_i(k) = q_k(i)$ für $i,k \in \{0,1,2,3\}$. Ein Assoziationsschema mit dieser Eigenschaft nennt man *selbstdual*.
Man sieht, dass das Berechnen der Eigenwerte und der idempotenten Basismatrizen Arbeit erfordert. Im Allgemeinen sind dies schwierige Probleme.

2 Das Assoziationsschema der symmetrischen Bilinearformen

In diesem Abschnitt schauen wir uns genauer das Assoziationsschema von symmetrischen Bilinearformen über einem Vektorraum der Dimension m über $\mathbb{F}_q$ an. Dabei sei $m \in \mathbb{N}$, $q = p^l$ für eine Primzahl $p \neq 2$ und ein $l \in \mathbb{N}$ und V stets ein m-dimensionaler Vektorraum über $\mathbb{F}_q$. Mit $X(m,q)$ bezeichnen wir den Vektorraum der symmetrischen Bilinearformen über V. Wir wiederholen zunächst einige Sätze über symmetrische Bilinearformen, die aus der (linearen) Algebra bekannt sind. Die Ergebnisse findet man etwa im Buch "Introduction to Quadratic Forms over Fields" von Lam [8].

2.1 Symmetrische Bilinearformen über $\mathbb{F}_q$

Definition. Eine Abbildung $b : V \times V \to \mathbb{F}_q$ heißt *symmetrische Bilinearform* über $\mathbb{F}_q$, falls gilt

(B1) $b(\lambda x + \mu y, z) = \lambda b(x,z) + \mu b(y,z)$ für alle $\lambda, \mu \in \mathbb{F}_q, x, y, z \in V$

(B2) $b(x,y) = b(y,x)$ für alle $x, y \in V$.

Ist $a_1, \ldots, a_n \in V$ eine Basis von V, so lässt sich jeder symmetrischen Bilinearform b von V eindeutig symmetrische Matrix B bezüglich $a_1, \ldots, a_n$ zuordnen durch

$$B := (b_{ij})_{1 \leq i,j \leq n}, \text{ wobei } b_{ij} := b(a_i, a_j),$$

genannt *Grammatrix* von b bezüglich $a_1, \ldots, a_n$. Dann gilt $b(x,y) = \widetilde{x}^T B \widetilde{y}$ für alle $x, y \in V$, wobei $\widetilde{x}$ bzw. $\widetilde{y}$ die Koordinaten von x bzw. y bezüglich $a_1, \ldots, a_n$ sind. Umgekehrt liefert jede symmetrische Matrix auf diese Weise eine symmetrische Bilinearform. $X(m,q)$ ist deshalb nach fester Basiswahl isomorph zu $Sym(m,q)$, dem Vektorraum der symmetrischen $(m \times m)$-Matrizen über $\mathbb{F}_q$.
Sei nun b eine symmetrische Bilinearform und seien $a_1, \ldots, a_n$ und $a'_1, \ldots, a'_n$ zwei Basen von V. Bezeichnen wir die Bilinearform auf den Koordinaten bezüglich $a_1, \ldots, a_n$ (also in $\mathbb{F}_q^m$) mit $\widetilde{b}$ und die Bilinearform auf den Koordinaten bezüglich $a'_1, \ldots, a'_n$ mit b', so gilt $b'(x,y) = \widetilde{b}(Sx, Sy)$, wobei $S \in GL(m,q)$ die Darstellungsmatrix des Basiswechsels von $a'_1, \ldots, a'_n$ nach $a_1, \ldots, a_n$ ist. Ist nun B die Grammatrix von b bezüglich der Basis $a_1, \ldots, a_n$, so ist die Grammatrix von b bezüglich $a'_1, \ldots, a'_n$ gegeben durch $S^T B S$. Da S regulär ist, sehen wir sofort, dass der Rang der Grammatrix invariant unter Basiswechseln ist. Wir definieren deshalb den *Rang* einer symmetrischen Bilinearform b

als den Rang einer beliebigen Grammatrix von b. Außerdem nennen wir zwei Matrizen $A, B \in Sym(m,q)$ *kongruent*, falls es ein $S \in GL(m,q)$ gibt, sodass $A = S^T BS$, und entsprechend nennen wir zwei Bilinearformen b, b' *isometrisch*, wenn es ein $S \in GL(V)$ gibt mit $b(x,y) = b'(S(x), S(y))$ für alle $x, y \in V$. Offenbar gilt:

2.1 Satz. *Zwei symmetrische Bilinearformen b, b' sind genau dann isometrisch, wenn ihre (bezüglich beliebiger Basen gebildeten) Grammatrizen kongruent sind.*

Es macht also keinen Unterschied, ob wir über kongruente Matrizen oder isometrische Bilinearformen reden. Aus der linearen Algebra zitieren wir weiter:

2.2 Theorem. *Es sei K ein Körper mit char $K \neq 2$. Zu jeder symmetrischen Bilinearform $b : V \times V \to K$ gibt es eine Basis $\widetilde{a_1}, \ldots, \widetilde{a_n}$ von V, bezüglich der die Grammatrix von b Diagonalgestalt hat.*

Dieses Resultat können wir für endliche Körper der Charakteristik ungleich 2, die wir in dieser Arbeit betrachten, verschärfen:

2.3 Theorem. *Ist $z \in \mathbb{F}_q^*$ ein fest gewähltes Nichtquadrat, so gibt es zu jeder symmetrischen Bilinearform b eine Basis $\mathcal{E}$ von V, sodass die Grammatrix B von b bezüglich $\mathcal{E}$ entweder die Nullmatrix ist, oder von der Form*

$$B = diag(1, 1, \ldots, 1, 0, \ldots, 0) \text{ oder } B = diag(z, 1, \ldots, 1, 0, \ldots, 0)$$

ist.

Dies sind also Vertreter für die Kongruenzklassen von $Sym(m,q)$. Jede symmetrische Matrix über $\mathbb{F}_q$ ist zu genau einer der oben angegebenen Vertreter kongruent.
Da bei einer diagonalisierten Form bei Skalierung eines einzelnen Basiselementes mit einem beliebigen Skalar $\lambda \neq 0$ nur der entsprechende Eintrag auf der Diagonalen mit λ^2 multipliziert wird, können wir dieses Theorem auch etwas anders formulieren:

2.4 Theorem. *Zu jeder symmetrischen Bilinearform b über V gibt es eine Basis $\mathcal{E}$ von V, sodass die Grammatrix B von b bezüglich $\mathcal{E}$ entweder die Nullmatrix ist, oder von der Form*

$$B = diag(z, 1, \ldots, 1, 0, \ldots, 0)$$

für ein Element $z \in \mathbb{F}_q^*$ ist.

Theorem (2.4) legt es nahe, das z auf der Diagonalen genauer zu betrachten. Theorem (2.3) liefert nun sofort die Wohldefiniertheit des folgendes Begriffs:

Definition. Sei $\eta : \mathbb{F}_q^* \to \{+1, -1\}$ der quadratische Charakter von $\mathbb{F}_q$, d.h.

$$\eta(x) = 1 \iff x \text{ ist ein Quadrat in } \mathbb{F}_q.$$

In der Situation von Theorem (2.4) nennt man dann $\eta(z)$ den *Typ* von b. Da ein leeres Produkt den Wert 1 hat, hat die Nullmatrix (bzw. die Nullform) Typ 1 (man fasse z als Produkt der Einträge ungleich 0 auf). Wir betonen hier nochmal, dass kongruente symmetrische Matrizen (beziehungsweise isometrische symmetrische Bilinearformen) denselben Rang und denselben Typ haben, und dass umgekehrt zwei symmetrische Bilinearformen von gleichem Rang und gleichem Typ isometrisch sind. Im Folgenden bezeichne η immer den quadratischen Charakter von $\mathbb{F}_q$.

2.2 Konstruktion des Assoziationsschemas

Wir folgen nun Kapitel 2 der Arbeit "Symmetric bilinear forms over finite fields with applications to coding theory" von Schmidt [12] und geben $X(m,q)$ die Struktur eines Assoziationsschemas, d.h. wir wählen $X := X(m,q)$ als Grundmenge und müssen nun geeignete Relationen definieren. Natürlich ist $X(m,q)$ endlich und enthält mindestens zwei Elemente und ist somit eine zulässige Grundmenge.
Um die Relationen zu definieren, betrachten wir zunächst eine Gruppenoperation auf X. Dazu sei G ein semidirektes Produkt von $GL(V)$ und X, in Zeichen $G := GL(V) \rtimes X$. Die Verknüpfung in G ist dabei wie folgt definiert:
Für $(S,A),(T,B) \in G$ ist $(S,A)(T,B) := (S \circ T, B' + A)$, wobei $B' \in X$ die Bilinearform ist, die durch $B'(x,y) := B(S(x),S(y))$ definiert ist, d.h. B und B' sind isometrisch. Im Folgenden schreiben wir nur kurz B', wenn klar ist, wie B' aussieht. Man beachte hier die Analogie zu beispielsweise der $AGL(V)$, die als semidirektes Produkt der $GL(V)$ mit $T(V)$, der Gruppe der Translationen in V, aufgefasst werden kann (dort haben wir $(S,v)(T,w) = (S \circ T, S(w) + v)$).
Es ist nicht schwer zu überprüfen, dass G tatsächlich eine Gruppe ist. Offenbar liegt die Verknüpfung zweier Elemente aus G wieder in G, $(id,0)$ ist das Neutralelement, und das Inverse zu (S,A) ist $(S^{-1},-\widetilde{A})$ mit $\widetilde{A}(x,y) = A(S^{-1}(x),S^{-1}(y))$. Man überzeugt sich auch leicht, dass in G das Assoziativgesetz gilt: Für $(S,A),(T,B),(U,C) \in G$ gilt

$$(S,A)((T,B)(U,C)) = (S,A)(T \circ U, C' + B) = (S \circ T \circ U, C'' + B' + A)$$

mit $C'(x,y) = C(T(x),T(y)), C''(x,y) = C((S \circ T)(x),(S \circ T)(y))$ und $B'(x,y) = B(S(x),S(y))$. Andererseits haben wir

$$((S,A)(T,B))(U,C) = (S \circ T, B' + A)(U,C) = (S \circ T \circ U, C'' + B' + A)$$

mit denselben C'', B'. Also ist G eine Gruppe. Nun operiert G auf X durch

$$\begin{aligned} G \times X &\to X \\ (S,A) \cdot B &:= B' + A, \end{aligned}$$

denn es gilt für jedes $F \in X$

$$(S,A) \cdot ((T,B) \cdot F) = (S,A) \cdot (F' + B) = F'' + B' + A$$

mit $F'(x,y) = F(T(x),T(y)), F''(x,y) = F((S \circ T)(x),(S \circ T)(y))$ und $B'(x,y) = B(S(x),S(y))$. Außerdem gilt

$$((S,A)(T,B)) \cdot F = (S \circ T, B' + A) \cdot F = F'' + B' + A$$

wieder mit $F''(x,y) = F((S \circ T)(x),(S \circ T)(y))$ und $B'(x,y) = B(S(x),S(y))$. Zusammen mit

$$(id,0) \cdot F = F' + 0 = F' = F,$$

da $F'(x,y) = F(id(x), id(y)) = F(x,y)$ gilt, erhalten wir, dass die gegebene Vorschrift eine Gruppenoperation von G auf X liefert.
Offenbar operiert G transitiv auf X, denn um $E \in X$ auf $F \in X$ abzubilden, wähle etwa $S = id$ und $A = F - E$. Dann gilt

$$(id, F-E) \cdot E = E' + (F-E) = E + F - E = F,$$

da wir genau wie zuvor $E' = E$ erhalten. Diese Operation lässt sich komponentenweise auf $X \times X$ fortsetzen und zerlegt somit $X \times X$ in Bahnen. Wir zeigen nun, dass diese Bahnen die Axiome für die Relationen eines Assoziationsschemas erfüllen:
Da $X \times X$ (die Grundmenge der Operation) die disjunkte Vereinigung aller Bahnen ist, ist (A0) erfüllt. Außerdem finden wir zu jedem $x \in X$ und jedem $y \in X$ ein $g \in G$ mit $g \cdot x = y$, weil G transitiv auf X operiert. Da die Operation auf $X \times X$ komponentenweise definiert ist, erhalten wir damit, dass $R_0 \coloneqq \{g \cdot (0,0) \mid g \in G\} = \{(g \cdot 0, g \cdot 0) \mid g \in G\} = \{(x,x) \mid x \in X\}$ eine Bahn ist, also gilt (A1). Auch (A2) ist sofort klar, denn die inverse Relation zur Bahn eines Elementes $(x,y) \in X \times X$ ist die Bahn des Elementes $(y,x) \in X \times X$, was wieder sofort aus der komponentenweisen Definition folgt.
Für Axiom (A3) müssen wir zeigen, dass die Schnittzahlen nicht von der speziellen Wahl der Vertreter abhängen. Seien dazu $i, j, k \in \{0, \ldots, d\}$, wobei d die Anzahl der Klassen des Schemas sei (diese werden wir gleich bestimmen), und $(x,y), (x',y') \in R_k$. Da G eingeschränkt auf eine Bahn transitiv operiert, gibt es ein $g \in G$ mit $g \cdot (x,y) = (x',y')$. Weil die Elemente von G wie bijektive Abbildungen auf X wirken, können wir jedem $z \in X$, das bezüglich (x,y) für die Schnittzahl gezählt werden muss, genau ein $z' \in X$ zuordnen, das wir bezüglich (x',y') zählen müssen, nämlich $z' = g \cdot z$. Denn haben wir $z \in X$ mit $(x,z) \in R_i$ und $(z,y) \in R_j$, so gilt auch $g \cdot (x,z) = (g \cdot x, g \cdot z) = (x', g \cdot z) \in R_i$ und $g \cdot (z,y) = (g \cdot z, g \cdot y) = (g \cdot z, y') \in R_j$, da die Relationen gerade die Bahnen der komponentenweisen Operation sind, d.h. durch Anwendung der Operation verlässt man die Bahn nicht. Die Elemente, die wir bezüglich (x,y) zählen müssen, lassen sich also mithilfe von g bijektiv auf die Elemente abbilden, die bezüglich (x',y') gezählt werden müssen. Also hängen die Schnittzahlen nur von den beteiligten Relationen ab, nicht aber von der Wahl der Vertreter. Damit ist (A3) gezeigt und $X(m,q)$ liefert mit den Bahnen der Operation ein Assoziationsschema.
Wir wollen nun die Relationen des Assoziationsschemas der symmetrischen Bilinearformen explizit beschreiben. Dazu definieren wir $X_{i,\tau}$ für jedes Paar $(i,\tau) \in \{1, \ldots, m\} \times \{+1, -1\}$ als die Menge aller symmetrischen Bilinearformen, die Rang i und Typ τ haben. Zusätzlich definieren wir noch $X_{0,1}$ als Menge, die nur die Nullform enthält (denn eine Bilinearform vom Rang 0 muss die Nullform sein und diese hat Typ 1, es wird also keine Menge $X_{0,-1}$ benötigt). Mithilfe der $X_{i,\tau}$ definieren außerdem die Relationen

$$R_{i,\tau} = \{(A,B) \in X \times X \mid A - B \in X_{i,\tau}\}$$

für jedes Paar (i,τ), für das die Menge $X_{i,\tau}$ definiert ist. Nun zeigen wir, dass die $R_{i,\tau}$ genau die Bahnen der Gruppenoperation, also genau die Relationen des Assoziationsschemas der symmetrischen Bilinearformen sind.
Dass die $R_{i,\tau}$ eine Partition von $X \times X$ bilden ist klar, denn die Differenz zweier Bilinearformen ist wieder eine Bilinearform, und diese hat entweder Rang 0 (liegt also in

$X_{0,1}$) oder Rang i und Typ τ für $i \in \{1, \ldots, m\}, \tau \in \{+1, -1\}$ und liegt damit genau in der Relation $R_{i,\tau}$. Man sieht auch leicht, dass Anwendung der Gruppenoperation die Mengen $R_{i,\tau}$ nicht verlässt. Denn ist $(A, B) \in R_{i,\tau}$ für beliebige i, τ und $(S, T) \in G$, so ist $A - B \in X_{i,\tau}$, und für $(S, T) \cdot (A, B) = (A' + T, B' + T)$ gilt

$$A' + T - (B' + T) = A' - B' = (A - B)' \in X_{i,\tau},$$

da $(A - B)'$ und $A - B$ isometrisch sind (Transformation mit S). Schließlich operiert G auch transitiv auf den $R_{i,\tau}$:
Sind $(A, B), (C, D) \in R_{i,\tau}$, so ist $A - B, C - D \in X_{i,\tau}$. Wir benötigen ein $g \in G$ mit $g \cdot (A, B) = (C, D)$. Nach Theorem (2.4) wissen wir, dass es ein $S \in GL(V)$ gibt mit $(A - B)' = (C - D)$, da die beiden Formen isometrisch sind. Damit gilt nun:

$$\begin{aligned}
(id, -B) \cdot (A, B) &= (A - B, B - B) = (A - B, 0) \\
(S, 0) \cdot (A - B, 0) &= ((A - B)' + 0, 0' + 0) = (C - D, 0) \\
(id, D) \cdot (C - D, 0) &= ((C - D) + D, 0 + D) = (C, D),
\end{aligned}$$

sodass $g \coloneqq (id, D)(S, 0)(id, -B) = (S, -B' + D) \in G$ das Gewünschte erfüllt. Damit sind die $R_{i,\tau}$ die Bahnen der Gruppenoperation und wir haben das Schema explizit beschrieben. Wir schreiben im Folgenden kurz $X(m, q)$ für das Assoziationsschema $(X(m, q), (R_{i,\tau}))$. Außerdem werden wir die Relationen weiterhin mit den Paaren (i, τ) und nicht mit den Zahlen von 0 bis d indizieren, da dies eine natürliche Nummerierung liefert.

2.3 Eigenschaften des Assoziationsschemas

In diesem Abschnitt geben wir einige Parameter von $X(m, q)$ an und definieren einige Ausdrücke und Hilfszahlen, die wir im Folgenden benötigen werden. Dabei folgen wir weiterhin Kapitel 2 in [12].
Zunächst sehen wir an der obigen Darstellung des Schemas mit den Relationen $R_{i,\tau}$, dass das Assoziationsschema $2m$ Klassen hat (denn die identische Relation $R_{0,1}$ wird nicht mitgezählt). Außerdem sieht man leicht, dass $X(m, q)$ für $q \equiv 1 \ mod \ 4$ symmetrisch ist. Denn dann ist -1 ein Quadrat in $\mathbb{F}_q$, d.h. es gibt ein $z \in \mathbb{F}_q^*$ mit $z^2 = -1$. Sei nun $(A, B) \in R_{i,\tau}$ für beliebige i und τ. Dann ist $A - B = -(B - A) = z^2(B - A)$. Da Skalieren einer Bilinearform mit einem Quadrat ungleich 0 eine isometrische Form liefert, ist auch $(B, A) \in R_{i,\tau}$. Also ist $X(m, q)$ symmetrisch (und damit nach (1.5) auch kommutativ).
Im Fall $q \equiv 3 \ mod \ 4$ ist das Schema zwar nicht mehr symmetrisch, da für $A, B \in X$ die Bilinearform $A - B$ nicht isometrisch zu $B - A$ ist, weil -1 kein Quadrat in $\mathbb{F}_q$ ist, aber immer noch kommutativ. Der Beweis ist allerdings lang und sehr rechenlastig, weshalb wir ihn hier nicht führen. Für einen Beweis siehe etwa Theorem 2 in [7]. Wir berechnen nun kurz die Valenz:

2.5 Satz. *Für alle i, τ gilt:*

$$v_{i,\tau} = |X_{i,\tau}|$$

Beweis. Seien i, τ beliebig. Nach (1.3) ist $v_{i,\tau}$ die Anzahl der $x \in X$ mit $(0, x) \in R_{i,\tau}$, d.h. $0 - x = -x \in X_{i,\tau}$, also $x \in -X_{i,\tau}$. Wegen $|-X_{i,\tau}| = |X_{i,\tau}|$ folgt die Behauptung. □

Wir wollen nun noch die (dualen) Eigenwerte von $X(m, q)$ angeben. Dazu benötigen wir einige Vorbereitungen.
Zunächst definieren wir für $n \in \mathbb{Z}$, $k \in \mathbb{N}_0$

$$\begin{bmatrix} n \\ k \end{bmatrix} := \prod_{i=1}^{k} \frac{q^{2(n-i+1)} - 1}{q^{2i} - 1}.$$

Dies ist nichts anderes als der Gauß-Koeffizient in q^2. Er erfüllt:

2.6 Lemma. *Für $n, k \in \mathbb{N}_0$ mit $n \geq k$ gilt*

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix} \text{ und } \begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1.$$

Beweis. Ohne Beschränkung der Allgemeinheit sei $k < \frac{n}{2}$. Ist $k = \frac{n}{2}$, so ist nichts zu zeigen. Ist $k > \frac{n}{2}$, so vertausche die Rollen von k und $n - k$.
Nach Definition ist

$$\begin{bmatrix} n \\ n-k \end{bmatrix} = \prod_{i=1}^{n-k} \frac{q^{2(n-i+1)} - 1}{q^{2i} - 1} = \left(\prod_{i=1}^{k} \frac{q^{2(n-i+1)} - 1}{q^{2i} - 1} \right) \left(\prod_{i=k+1}^{n-k} \frac{q^{2(n-i+1)} - 1}{q^{2i} - 1} \right).$$

Dies können wir wegen $k < \frac{n}{2}$ auf diese Weise auftrennen, sodass wir nach Definition des Gauß-Koeffizienten nur noch zeigen müssen, dass das zweite Produkt den Wert 1 hat. Wir sehen, dass der Exponent von q^2 im Zähler die Zahlen

$$n - k,\ n - k - 1,\ \ldots k + 1$$

durchläuft. Dies sind genau die Exponenten von q^2 im Nenner in umgekehrter Reihenfolge. Also ist das Produkt der Zähler gleich dem Produkt der Nenner und damit hat das hintere Produkt den Wert 1.
Weiterhin ist sofort ersichtlich, dass das Produkt für $k = 0$ leer, also gleich 1 ist. Mit

$$\begin{bmatrix} n \\ n \end{bmatrix} = \begin{bmatrix} n \\ n-n \end{bmatrix} = \begin{bmatrix} n \\ 0 \end{bmatrix} = 1$$

folgt die Behauptung. □

Außerdem definieren wir folgende Hilfszahlen

$$F_r^{(m)}(s) := \sum_{j=0}^{r} (-1)^{r-j} q^{(r-j)(r-j-1)} \begin{bmatrix} n-j \\ n-r \end{bmatrix} \begin{bmatrix} n-s \\ j \end{bmatrix} c^j,$$

wobei

$$n := \left\lfloor \frac{m}{2} \right\rfloor \text{ und } c := q^{m(m-1)/(2n)},$$

überall, wo dieser Ausdruck definiert ist, und $F_r^{(m)}(s) := 0$ sonst. Diese Zahlen kommen von sogenannten *verallgemeinerten Krawtchouk-Polynomen*. Sie treten des Öfteren im Zusammenhang mit Assoziationsschemata auf. So sind zum Beispiel die Eigenwerte des Hamming-Schemas gegeben als Auswertung (nicht verallgemeinerter) Krawtchouk-Polynome (siehe dazu Theorem 5 in Kapitel 21 in [10]).
Sei $\chi : \mathbb{F}_q \to \mathbb{C}^*$ ein nicht trivialer Charakter von $(\mathbb{F}_q, +)$, d.h. $\chi(x+y) = \chi(x)\chi(y)$ für alle $x, y \in \mathbb{F}_q$. Dann definieren wir

$$\gamma_q := \sum_{x \in \mathbb{F}_q^*} \eta(x)\chi(x).$$

Dies ist eine sogenannte *quadratische Gauß-Summe*, welche explizit berechnet werden kann (siehe dafür etwa Theorem 5.12 in [9]). Der genaue Wert ist für uns aber nicht relevant. Wir können nun die dualen Eigenwerte angeben:

2.7 Theorem. [12, Theorem 2.2] *Die dualen Eigenwerte von $X(m,q)$ sind $Q_{0,1}(i,\tau) = 1$ für alle i und τ, $Q_{k,\epsilon}(0,1) = v_{k,\epsilon}$ für alle k und ϵ, und für $k, i \geq 1$ und $\tau, \epsilon \in \{+1, -1\}$ ist $Q_{k,\epsilon}(i,\tau)$ gegeben durch*

$$\begin{aligned}
2Q_{2r+1,\epsilon}(2s+1,\tau) &= -q^{2r}F_r^{(m-1)}(s) + \epsilon\tau\eta(-1)^{s+r}q^{m-s+r-1}\gamma_q F_r^{(m-1)}(s),\\
2Q_{2r,\epsilon}(2s+1,\tau) &= q^{2r}F_r^{(m-1)}(s) + \epsilon\eta(-1)^r q^r F_r^{(m)}(s),\\
2Q_{2r+1,\epsilon}(2s,\tau) &= -q^{2r}F_r^{(m-1)}(s-1) + \tau\eta(-1)^s q^{m-s+2r}F_r^{(m-2)}(s-1),\\
2Q_{2r,\epsilon}(2s,\tau) &= q^{2r}F_r^{(m-1)}(s-1) - \tau\eta(-1)^s q^{m-s+2r-2}F_{r-1}^{(m-2)}(s-1)\\
&\quad + \epsilon\eta(-1)^r q^r F_r^{(m)}(s).
\end{aligned}$$

Der Beweis ist lang und schwierig. Man findet ihn in Anhang B in [12].

2.8 Bemerkung. Man beachte, dass Theorem (2.7) von der Wahl des Charakters χ abhängt, da dieser in die quadratische Gauß-Summe eingeht. Die Wahl eines anderen Charakters kann den Wert von γ_q ändern und hat damit nach Theorem (2.7) Einfluss auf die Zahlen $Q_{2r+1,\epsilon}(2s+1,\tau)$. Durch einen anderen Charakter können die Rollen von $Q_{2r+1,1}(2s+1,\tau)$ und $Q_{2r+1,-1}(2s+1,\tau)$ vertauscht werden, d.h. die Reihenfolge der idempotenten Basismatrizen kann sich ändern.
Man kann außerdem zeigen, dass für die Eigenwerte $P_{i,\tau}(k,\epsilon)$ gilt

$$P_{i,\tau}(k,\epsilon) = \overline{Q_{k,\epsilon}(i,\tau)} \text{ für alle } i, \tau, k, \epsilon.$$

Mit Theorem (2.7) erhalten wir also nicht nur die dualen, sondern direkt auch die gewöhnlichen Eigenwerte.

3 Codes und Designs

In diesem Kapitel wollen wir Teilmengen eines Assoziationsschemas genauer untersuchen. Dazu definieren wir sogenannte d-Codes und t-Designs und schauen uns an, was diese mit den aus der Codierungstheorie bekannten Codes zu tun haben. Grundbegriffe der Codierungstheorie sind dem Buch von MacWilliams und Sloane entnommen [10].

3.1 Codes und Designs

Dieser Abschnitt richtet sich nach Teilen von Abschnitt 7 in Kapitel 21 in [10] und Kapitel 3 in [4].

Definition. Sei (X, R) ein Assoziationsschema mit n Klassen und $\emptyset \neq Y \subseteq X$. Dann heißen die Zahlen

$$a_i := \frac{1}{|Y|} \left| (Y \times Y) \cap R_i \right| , \; i = 0, \ldots, n,$$

die *innere Verteilung* von Y. Anschaulich beschreibt a_i die durchschnittliche Anzahl von Elementen $z \in Y$, die zu einem Element $y \in Y$ in Relation i stehen. Gilt dabei

$$a_1 = a_2 = \ldots = a_{d-1} = 0$$

für ein $d \in \{1, \ldots, n\}$, so nennt man Y *d-Code*. Man beachte, dass in der Definition eines d-Codes nicht gefordert wird, dass $a_d \neq 0$ gilt, d.h. ein d-Code ist auch ein d'-Code für jedes $d' \leq d$.

Natürlich hängt der Begriff des d-Codes von der Nummerierung der Relationen ab. In den meisten konkreten Beispielen (wie etwa dem Hamming-Schema) hat man allerdings eine natürliche Indizierung der Relationen gegeben, bezüglich der der Begriff des d-Codes sinnvoll ist (siehe dazu (3.2)). Wir geben zunächst einige einfache Eigenschaften der inneren Verteilung an:

3.1 Lemma. *Die innere Verteilung $(a_i)_{i=0}^n$ eines Assoziationsschemas (X, R) erfüllt:*

(a) $a_0 = 1$

(b) $a_i \geq 0$ *für alle* $i = 0, \ldots, n$

(c) $\sum_{i=0}^{n} a_i = |Y|$

Beweis. Zu (a): Klar, da $|(Y \times Y) \cap R_0| = |\{(y, y) \mid y \in Y\}| = |Y|$.
Zu (b): Trivial.
Zu (c): Da die R_i disjunkt sind, sind sie es natürlich auch noch nach Schnitt mit $(Y \times Y)$, also gilt

$$\begin{aligned}
\sum_{i=0}^{n} a_i &= \frac{1}{|Y|} \sum_{i=0}^{n} |\, R_i \cap (Y \times Y)\,| \\
&= \frac{1}{|Y|} \left| \bigcup_{i=0}^{n} (R_i \cap (Y \times Y)) \right| \\
&= \frac{1}{|Y|} \left| \left(\bigcup_{i=0}^{n} R_i \right) \cap (Y \times Y) \right| \\
&= \frac{1}{|Y|} |\,(Y \times Y)\,| = |Y|. \qquad \square
\end{aligned}$$

3.2 Bemerkung. Der Begriff d-Code für eine Teilmenge Y mit $a_1 = \ldots = a_{d-1} = 0$ ist dadurch gerechtfertigt, dass ein (nicht notwendig linearer) Code der Länge n über $\mathbb{F}_q$ im Sinne der Codierungstheorie nichts anderes ist als eine Teilmenge des Hamming-Schemas $H(q, n)$. Ist nämlich $Y \subseteq \mathbb{F}_q^n$, so gilt:

$$\begin{aligned}
&Y \text{ ist ein } d\text{-Code im Sinne der Assoziationsschemata} \\
\iff\ &Y \text{ ist ein Code im Sinne der Codierungstheorie mit Minimalabstand } \geq d,
\end{aligned}$$

denn $a_1 = \ldots = a_{d-1} = 0$ bedeutet, dass Y keine Elemente enthält, die in Relation R_i stehen für $i = 1, \ldots, d-1$. Für das Hamming-Schema heißt das dann, dass Y keine Elemente vom Hammingabstand kleiner als d enthält. Der Minimalabstand des Codes Y ist also mindestens d. Das Problem, einen für gegebenes n und d möglichst großen (n, M, d)-Code über $\mathbb{F}_q$ zu finden, lässt sich somit direkt auf das Problem, einen möglichst großen d-Code in $H(q, n)$ zu finden, übersetzen.
Allgemeiner lässt sich der Begriff d-Code besonders gut in sogenannten *metrischen* Assoziationsschemata interpretieren, die in Kapitel 5.2 in [4] genauer untersucht werden. Dabei bezeichnet man ein Assoziationsschema (X, R) mit n Klassen als *metrisch*, falls die Abbildung

$$\rho : X \times X \to \{0, \ldots, n\},\ \rho(x, y) = k :\Leftrightarrow (x, y) \in R_k$$

eine Metrik ist, und zusätzlich noch folgende Eigenschaft hat:
Sind $x, y \in X$ mit $\rho(x, y) = k$ für ein $k \in \{1, \ldots, n\}$, so gibt es ein $z \in X$ mit $\rho(x, z) = 1$ und $\rho(z, y) = k-1$. Dies schließt einige degenerierte Fälle aus. Offenbar ist das Hamming-Schema $H(q, n)$ nach Definition metrisch.

Mithilfe einer weiteren Verteilung kann man ein Analogon zum Begriff des d-Codes erhalten:

3.3 Satz und Definition. *Sei (X, R) ein Assoziationsschema mit n Klassen. Die* duale Verteilung *einer nichtleeren Teilmenge Y von X ist definiert als*

$$a'_k := \frac{1}{|Y|} \sum_{i=0}^{n} q_k(i) a_i$$

für $k = 0, \ldots, n$. Gilt dabei

$$a'_1 = a'_2 = \ldots = a'_t = 0$$

für ein $t \in \{1, \ldots, n\}$, so nennt man Y ein t-Design. Man beachte, dass wir im Gegensatz zum Begriff des d-Codes für ein t-Design auch $a'_t = 0$ fordern. Allerdings gilt wieder, dass $a'_{t+1} \neq 0$ nicht gefordert wird . Die duale Verteilung ist reell und nicht negativ.

Beweis. Betrachte den Spaltenvektor $u \in \mathbb{C}^{|X|}$ mit

$$u_x := \begin{cases} 1, & \text{falls } x \in Y \\ 0, & \text{falls } x \notin Y \end{cases},$$

also den charakteristischen Vektor von Y. Dann gilt

$$a_i = \frac{1}{|Y|} u^T A_i u,$$

denn der Eintrag $(A_i u)_x$ zählt die Anzahl der $y \in Y$ mit $(x, y) \in R_i$. Der Ausdruck $u^T(A_i u)$ summiert also alle Anzahlen der Paare auf, für die $x \in Y$ gilt, also $u^T A_i u = |R_i \cap (Y \times Y)|$. Damit folgt nach Definition der Eigenwerte

$$\begin{aligned} a'_k &= \frac{1}{|Y|} \sum_{i=0}^{n} q_k(i) a_i \\ &= \frac{1}{|Y|} \sum_{i=0}^{n} q_k(i) \left(\frac{1}{|Y|} u^T A_i u \right) \\ &= \frac{1}{|Y|^2} u^T \left(\sum_{i=0}^{n} q_k(i) A_i \right) u \\ &= \frac{1}{|Y|^2} u^T \left(|X| E_k \right) u. \end{aligned}$$

Da die E_i idempotent sind, können sie nur die Eigenwerte 0 und 1 haben. Damit sind sie positiv semidefinit, weil sie nach Satz (1.15) hermitesch sind, also folgt $a'_k \geq 0$ für jedes $k = 0, \ldots, n$. □

Die Darstellungen

$$a_i = \frac{1}{|Y|} u^T A_i u \quad \text{und} \quad a'_k = \frac{|X|}{|Y|^2} u^T E_k u$$

zeigen, wie eng die beiden Begriffe miteinander verbunden sind, und rechtfertigen die Bezeichnung "duale Verteilung".

Der Begriff des t-Designs lässt sich nicht allgemein interpretieren. In den meisten Fällen lässt sich aber eine "schöne" kombinatorische Interpretation angeben. Um den Begriff Design zu rechtfertigen, müssen wir das *Johnson-Schema* definieren:

Definition. Das *Johnson-Schema* $J(v,n)$ ist eine Teilmenge des binären Hamming-Schemas $H(2,n)$. Seine Grundmenge ist die Menge $S_n^v := \{x \in \mathbb{F}_2^v \mid w(x) = n\}$, wobei $w(x)$ das Hamminggewicht von x bezeichnet, also $w(x) = d(x,0)$. Da S_n^v und S_{v-n}^v durch Translation mit dem Einsvektor ineinander übergehen, können wir ohne Beschränkung der Allgemeinheit $0 \leq n \leq \lfloor \frac{v}{2} \rfloor$ annehmen. Die Relationen R_i $(i = 0, \ldots, n)$ des Johnson-Schemas sind definiert durch

$$R_i := \{(x,y) \in S_n^v \times S_n^v \mid d(x,y) = 2i\}.$$

Dass $J(v,n)$ ein symmetrisches Assoziationsschema ist, folgt genau wie beim Hamming-Schema. Wir gehen nur kurz auf (A0) ein:
Für $x, y \in \mathbb{F}_2^v$ gilt:

$$d(x,y) = d(x+y,0) = w(x+y) = w(x) + w(y) - 2w(x*y) = 2n - 2w(x*y),$$

wobei $x*y$ das komponentenweise Produkt von x und y bezeichnet. Also ist $d(x,y)$ für alle $x, y \in S_n^v$ eine gerade Zahl zwischen 0 und $2n$, sodass die Relationen tatsächlich eine Partition von $S_n^v \times S_n^v$ bilden.
Wir erinnern kurz an den Begriff eines $t-(v,k,\lambda)$-(Block)designs:

Definition. Ein Paar $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ bestehend aus einer Menge $\mathcal{P}$ mit $|\mathcal{P}| = v$ und einer Menge $\mathcal{B}$ bestehend aus k-elementigen Teilmengen von $\mathcal{P}$ mit $1 \leq k < v$ heißt $t-(v,k,\lambda)$-Design $(1 \leq \lambda, 1 \leq t \leq k)$, wenn gilt:
Jede t-elementige Teilmenge von $\mathcal{P}$ liegt in genau λ Mengen von $\mathcal{B}$.

Damit können wir die Interpretation von t-Designs im Johnson-Schema angeben:

3.4 Bemerkung. [4, Theorem 4.7] Eine Teilmenge $Y \subseteq S_n^v$ des Johnson-Schemas ist ein t-Design im Sinne der Assoziationsschemata genau dann, wenn Y ein $t-(v,n,\lambda)$-Design für ein passendes λ ist, wobei die Vektoren aus Y als Inzidenzvektoren der Blöcke interpretiert und so mit ihnen assoziiert werden.

t-Designs in anderen Assoziationsschemata können ganz andere, von Blockdesigns unabhängige Interpretationen haben.

3.2 Codes und Designs in $X(m,q)$

In diesem Abschnitt gehen wir genauer auf das Assoziationsschema der symmetrischen Bilinearformen über $\mathbb{F}_q$ ein. Zunächst müssen wir die Begriffe aus dem vorherigen Abschnitt für $X(m,q)$ neu definieren, da diese leicht von der obigen (allgemein üblichen) Definition abweichen. Die innere Verteilung für Teilmengen von $X(m,q)$ unterscheidet sich nicht von der für andere Assoziationsschemata (lediglich die Indizierung ist anders),

aber die duale Verteilung definieren wir ohne den Vorfaktor. Dies macht einige Rechnungen etwas schöner. Codes und Designs beziehen sich hier nur auf den Rang, *nicht* auf den Typ. Sätze und Definitionen in diesem Abschnitt sind Abschnitt 1 in Kapitel 3 in [12] entnommen.

Definition. Ist $Y \subseteq X(m,q)$ und $(a_{i,\tau})$ die innere Verteilung von Y, so nennen wir die Zahlen

$$a'_{k,\epsilon} := \sum_{i,\tau} Q_{k,\epsilon}(i,\tau) a_{i,\tau}$$

die *duale Verteilung* von Y.
Y heißt *d-Code* für ein $d \in \{1,\dots,n\}$, falls gilt

$$a_{1,1} = a_{1,-1} = \dots = a_{d-1,1} = a_{d-1,-1} = 0.$$

Y heißt t-Design für ein $t \in \{1,\dots,n\}$, falls gilt

$$a'_{1,1} = a'_{1,-1} = \dots = a'_{t,1} = a'_{t,-1} = 0.$$

Versehen wir $X(m,q)$ mit der Funktion $\rho : X(m,q) \times X(m,q) \to \{0,\dots,n\}$, $\rho(A,B) = \mathrm{Rang}(A-B)$, so können wir d-Codes wieder direkt mit codierungstheoretischen Codes in Beziehung setzen. Denn offenbar gilt für alle $A,B,C \in X(m,q)$

$$\begin{aligned}
&\rho(A,B) = 0 \iff \mathrm{Rang}(A-B) = 0 \iff A-B = 0 \iff A = B,\\
&\rho(A,B) = \mathrm{Rang}(A-B) = \mathrm{Rang}(B-A) = \rho(B,A),\\
&\rho(A,C) = \mathrm{Rang}(A-C) = \mathrm{Rang}(A-B+B-C)\\
&\qquad \le \mathrm{Rang}(A-B) + \mathrm{Rang}(B-C) = \rho(A,B) + \rho(B,C).
\end{aligned}$$

Also ist ρ eine Metrik. Auch t-Designs haben eine kombinatorische Interpretation, wir geben sie hier ohne Beweis an. Wir erinnern noch einmal daran, dass $X(m,q)$ die Menge der symmetrischen Bilinearformen ist, die auf einem m-dimensionalen Vektorraum $V(m,q)$ über $\mathbb{F}_q$ definiert sind.

3.5 Bemerkung. [12, Theorem 3.11] Sei U ein t-dimensionaler Untervektorraum von $V(m,q)$ und A eine symmetrische Bilinearform auf U. Eine Teilmenge Y von $X(m,q)$ ist genau dann ein t-Design, wenn die Anzahl an Formen in Y, die eine Erweiterung von A sind (d.h. die Anzahl an Formen in Y, deren Einschränkung auf U gleich A ist), unabhängig von der Wahl von U und A ist.

Nun geben wir noch Systeme von Zahlen A_s, B_s, C_s, D_s sowie A'_r, B'_r, C'_r, D'_r an, die die folgenden Rechnungen leichter machen, und die sich ähnlich wie die innere bzw. duale Verteilung verhalten.

Definition. Ist $(a_{i,\tau})$ die innere Verteilung einer Teilmenge Y von $X(m,q)$ und $(a'_{k,\epsilon})$ ihre duale Verteilung, so definieren wir für $s,r \in \{0,\dots,\lfloor \frac{m}{2} \rfloor\}$

$$\begin{aligned}
A_s &:= a_{2s,1} + a_{2s,-1} + a_{2s-1,1} + a_{2s-1,-1},\\
B_s &:= a_{2s,1} + a_{2s,-1} + a_{2s+1,1} + a_{2s+1,-1},\\
C_s &:= \eta(-1)^s q^{-s}(a_{2s,1} - a_{2s,-1}),\\
D_s &:= \eta(-1)^s q^{-s}(a_{2s+1,1} - a_{2s+1,-1})
\end{aligned}$$

und

$$\begin{aligned}
A'_r &:= a'_{2r,1} + a'_{2r,-1} + a'_{2r-1,1} + a'_{2r-1,-1},\\
B'_r &:= a'_{2r,1} + a'_{2r,-1} + a'_{2r+1,1} + a'_{2r+1,-1},\\
C'_r &:= \eta(-1)^r q^{-r}(a'_{2r,1} - a'_{2r,-1}),\\
D'_r &:= \eta(-1)^r q^{-r}(a'_{2r+1,1} - a'_{2r+1,-1}).
\end{aligned}$$

Wir erinnern noch einmal daran, dass wir $a_{i,\tau}$ und $a'_{k,\epsilon}$ auf 0 setzen, falls diese nicht definiert sind.

Man sieht leicht, dass die Kenntnis der Zahlen $(A_s),(B_s),(C_s)$ und (D_s) äquivalent zur Kenntis der inneren Verteilung ist. Denn diese Zahlen berechnen sich aus der inneren Verteilung und umgekehrt lässt sich die innere Verteilung wieder aus den Zahlen $(A_s),(B_s),(C_s)$ und (D_s) zurückgewinnen:
Zunächst haben wir $A_0 = C_0 = a_{0,1}$. Dies können wir dann aus $B_0 = a_{0,1} + a_{1,1} + a_{1,-1}$ herauskürzen und erhalten mit $D_0 = a_{1,1} - a_{1,-1}$ zwei linear unabhängige Gleichungen für $a_{1,1}$ und $a_{1,-1}$, aus denen wir diese bestimmen können. Wenn $a_{1,1}$ und $a_{1,-1}$ nun bekannt sind, können wir sie aus $A_1 = a_{2,1} + a_{2,-1} + a_{1,1} + a_{1,-1}$ herauskürzen und erhalten mit $C_1 = \eta(-1)^1 q^{-1}(a_{2,1} - a_{2,-1})$ wieder zwei linear unabhängige Gleichungen für $a_{2,1}$ und $a_{2,-1}$. Diese können wir nun benutzen, um aus $B_1 = a_{2,1} + a_{2,-1} + a_{3,1} + a_{3,-1}$ und $D_1 = \eta(-1)^1 q^{-1}(a_{3,1} - a_{3,-1})$ die nächsten beiden Zahlen $a_{3,1}$ und $a_{3,-1}$ zu bestimmen. Sind also im Allgemeinen alle $a_{i,\tau}$ bis $i = h$ bestimmt, so erhält man $a_{h+1,1}$ und $a_{h+1,-1}$ aus $A_{\frac{h+1}{2}}$ und $C_{\frac{h+1}{2}}$, falls $h+1$ gerade ist, und aus $B_{\frac{h}{2}}$ und $D_{\frac{h}{2}}$, falls $h+1$ ungerade ist (also h gerade ist). Iterativ erhält man so aus den Zahlen $(A_s),(B_s),(C_s)$ und (D_s) die innere Verteilung $(a_{i,\tau})$ zurück. Da die Zahlen $(A'_r),(B'_r),(C'_r)$ und (D'_r) vollkommen analog definiert sind, gilt dasselbe auch für die duale Verteilung $(a'_{k,\epsilon})$.
Der Grund für die Einführung dieser Zahlen ist folgender Satz:

3.6 Satz. [12, Lemma 3.2] *Sei $\emptyset \neq Y \subseteq X(m,q)$ und seien die Zahlen A_s, B_s, C_s und D_s sowie A'_r, B'_r, C'_r und D'_r wie oben mithilfe der inneren und dualen Verteilung definiert.*

Dann gilt mit $n := \lfloor \frac{m}{2} \rfloor$

$$\begin{aligned} A'_r &= \sum_{s=0}^{n} F_r^{(m+1)}(s) A_s, \\ B'_r &= q^m \sum_{s=0}^{n} F_r^{(m)}(s) C_s, \\ C'_r &= \sum_{s=0}^{n} F_r^{(m)}(s) B_s, \\ D'_r &= q^{m-1} \gamma_q \sum_{s=0}^{n} F_r^{(m-1)}(s) D_s. \end{aligned}$$

Dabei ist γ_q *wieder die quadratische Gauß-Summe, die auch schon in (2.7) vorkam.*

Um (3.6) zu beweisen, benötigen wir folgende Rechenregel für den Gauß-Koeffizienten in q^2:

3.7 Lemma. *Für* $n \in \mathbb{Z}, k \in \mathbb{N}_0$ *(nicht beide gleichzeitig 0) gilt*

$$\begin{bmatrix} n \\ k \end{bmatrix} = q^{2k} \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} = \begin{bmatrix} n-1 \\ k \end{bmatrix} + q^{2(n-k)} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}.$$

Für den Fall $k = 0$ *setzen wir dabei*

$$\begin{bmatrix} n-1 \\ -1 \end{bmatrix} = 0.$$

Beweis. Wir erinnern zunächst nochmal an die Definition des Gauß-Koeffizienten in q^2:

$$\begin{bmatrix} n \\ k \end{bmatrix} := \prod_{i=1}^{k} \frac{q^{2(n-i+1)} - 1}{q^{2i} - 1}$$

Den Fall $k = 0$ erhalten wir sofort aus Satz (2.6). Wir zeigen nun die erste Gleichheit. Seien dazu $n \in \mathbb{Z}$ und $k \in \mathbb{N}$ beliebig. Dann gilt

$$\begin{aligned} & q^{2k} \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} = q^{2k} \prod_{i=1}^{k} \frac{q^{2((n-1)-i+1)} - 1}{q^{2i} - 1} + \prod_{i=1}^{k-1} \frac{q^{2((n-1)-i+1)} - 1}{q^{2i} - 1} \\ &= q^{2k} \prod_{i=1}^{k} \frac{q^{2(n-i)} - 1}{q^{2i} - 1} + \prod_{i=1}^{k} \frac{q^{2(n-i)} - 1}{q^{2i} - 1} \cdot \frac{q^{2k} - 1}{q^{2(n-k)} - 1} \\ &= \prod_{i=1}^{k} \frac{q^{2(n-i)} - 1}{q^{2i} - 1} \cdot \left(q^{2k} + \frac{q^{2k} - 1}{q^{2(n-k)} - 1} \right) \\ &= \prod_{i=1}^{k} \frac{q^{2(n-i)} - 1}{q^{2i} - 1} \cdot \left(\frac{q^{2n} - q^{2k}}{q^{2(n-k)} - 1} + \frac{q^{2k} - 1}{q^{2(n-k)} - 1} \right). \end{aligned}$$

Wir ändern nun die Indizierung des Produktes der Zähler um 1 und gleichen dies durch Ergänzen und Wegkürzen der Randterme aus. An den Nennern ändern wir nichts. Damit erhalten wir

$$\left(\prod_{i=1}^{k}\frac{q^{2(n-i+1)}-1}{q^{2i}-1}\right)\cdot\frac{q^{2(n-k)}-1}{q^{2n}-1}\cdot\frac{q^{2n}-1}{q^{2(n-k)}-1}=\prod_{i=1}^{k}\frac{q^{2(n-i+1)}-1}{q^{2i}-1}=\begin{bmatrix}n\\k\end{bmatrix},$$

was zu zeigen war.
Für die zweite Gleichung vertauschen wir mit Lemma (2.6) die Rollen von k und $n-k$ und benutze die bereits bewiesene Identität. Wir erhalten

$$\begin{bmatrix}n\\k\end{bmatrix}=\begin{bmatrix}n\\n-k\end{bmatrix}=q^{2(n-k)}\begin{bmatrix}n-1\\n-k\end{bmatrix}+\begin{bmatrix}n-1\\n-k-1\end{bmatrix}=\begin{bmatrix}n-1\\k\end{bmatrix}+q^{2(n-k)}\begin{bmatrix}n-1\\k-1\end{bmatrix}.$$

□

Nun können wir Satz (3.6) beweisen:

Beweis. Wir haben

$$A'_r=a'_{2r,1}+a'_{2r,-1}+a'_{2r-1,1}+a'_{2r-1,-1}\ \text{ und }\ A_s=a_{2s,1}+a_{2s,-1}+a_{2s-1,1}+a_{2s-1,-1}$$

und nach Definition der dualen Verteilung gilt

$$a'_{i,\tau}=\sum_{k,\epsilon}Q_{i,\tau}(k,\epsilon)a_{k,\epsilon}.$$

Folglich

$$\begin{aligned}A'_r&=a'_{2r,1}+a'_{2r,-1}+a'_{2r-1,1}+a'_{2r-1,-1}\\&=\sum_{k,\epsilon}Q_{2r,1}(k,\epsilon)a_{k,\epsilon}+\sum_{k,\epsilon}Q_{2r,-1}(k,\epsilon)a_{k,\epsilon}+\\&\quad\sum_{k,\epsilon}Q_{2r-1,1}(k,\epsilon)a_{k,\epsilon}+\sum_{k,\epsilon}Q_{2r-1,-1}(k,\epsilon)a_{k,\epsilon}\\&=\sum_{k,\epsilon}(Q_{2r,1}(k,\epsilon)+Q_{2r,-1}(k,\epsilon)+Q_{2r-1,1}(k,\epsilon)+Q_{2r-1,-1}(k,\epsilon))a_{k,\epsilon}.\end{aligned}$$

Wir berechnen nun für jedes Paar (i,τ) die Summe der vier Eigenwerte. Bei Rechnungen dieser Art betrachten wir im Folgenden immer zunächst die doppelte Summe, um nicht durch 2 teilen zu müssen. Theorem (2.7) liefert uns für gerades $i=2s\neq 0$ und $\tau\in\{+1,-1\}$

$$\begin{aligned}&2Q_{2r,1}(i,\tau)+2Q_{2r,-1}(i,\tau)+2Q_{2r-1,1}(i,\tau)+2Q_{2r-1,-1}(i,\tau)\\=\;&q^{2r}F_r^{(m-1)}(s-1)-\tau\eta(-1)^sq^{m-s+2r-2}F_{r-1}^{(m-2)}(s-1)+\eta(-1)^rq^rF_r^{(m)}(s)\\&+q^{2r}F_r^{(m-1)}(s-1)-\tau\eta(-1)^sq^{m-s+2r-2}F_{r-1}^{(m-2)}(s-1)-\eta(-1)^rq^rF_r^{(m)}(s)\\&-q^{2(r-1)}F_{r-1}^{(m-1)}(s-1)+\tau\eta(-1)^sq^{m-s+2(r-1)}F_{r-1}^{(m-2)}(s-1)\\&-q^{2(r-1)}F_{r-1}^{(m-1)}(s-1)+\tau\eta(-1)^sq^{m-s+2(r-1)}F_{r-1}^{(m-2)}(s-1)\\=\;&2q^{2r}F_r^{(m-1)}(s-1)-2q^{2(r-1)}F_{r-1}^{(m-1)}(s-1),\end{aligned}$$

sodass die ursprüngliche Summe den Wert $q^{2r}F_r^{(m-1)}(s-1)-q^{2(r-1)}F_{r-1}^{(m-1)}(s-1)$ hat. Mit der Definition der Zahlen $F_r^{(m)}(s)$ können wir dies weiter umformen. Da die Konstanten n und c (nur) von der Dimension m des zugrundeliegenden Vektorraumes abhängen, schreiben wir für sie der Deutlichkeit halber n_m und c_m. Es folgt

$$\begin{aligned}
&q^{2r}F_r^{(m-1)}(s-1) - q^{2(r-1)}F_{r-1}^{(m-1)}(s-1)\\
&= q^{2r}\sum_{j=0}^{r}(-1)^{r-j}q^{(r-j)(r-j-1)}\begin{bmatrix} n_{m-1}-j \\ n_{m-1}-r\end{bmatrix}\begin{bmatrix} n_{m-1}-(s-1) \\ j\end{bmatrix}c_{m-1}^j -\\
&\quad q^{2(r-1)}\sum_{j=0}^{r-1}(-1)^{r-1-j}q^{(r-1-j)(r-1-j-1)}\begin{bmatrix} n_{m-1}-j \\ n_{m-1}-r+1\end{bmatrix}\begin{bmatrix} n_{m-1}-(s-1) \\ j\end{bmatrix}c_{m-1}^j\\
&= \sum_{j=0}^{r}q^{2j}q^{2(r-j)}(-1)^{r-j}q^{(r-j)(r-j-1)}\begin{bmatrix} n_{m-1}-j \\ n_{m-1}-r\end{bmatrix}\begin{bmatrix} n_{m-1}+1-s \\ j\end{bmatrix}c_{m-1}^j +\\
&\quad \sum_{j=0}^{r}q^{2j}q^{2(r-j-1)}(-1)^{r-j}q^{(r-j-1)(r-j-2)}\begin{bmatrix} n_{m-1}-j \\ n_{m-1}-r+1\end{bmatrix}\begin{bmatrix} n_{m-1}+1-s \\ j\end{bmatrix}c_{m-1}^j\\
&= \sum_{j=0}^{r}(-1)^{r-j}q^{(r-j)(r-j-1)}\begin{bmatrix} n_{m-1}+1-s \\ j\end{bmatrix}q^{2j}c_{m-1}^j\left(q^{2(r-j)}\begin{bmatrix} n_{m-1}-j \\ n_{m-1}-r\end{bmatrix}+\begin{bmatrix} n_{m-1}-j \\ n_{m-1}-r+1\end{bmatrix}\right).
\end{aligned}$$

Wir konnten die zweite Summe anstatt bis $r-1$ ohne Probleme bis r gehen lassen, da der Summand für $j=r$ wegen

$$\begin{bmatrix} n \\ k\end{bmatrix} = 0 \text{ für } n<k$$

Null wird. Das liegt daran, dass in der Definition des Gauß-Koeffizienten der Zähler des Faktors für $i=n+1$ (der wegen $n<k$ auftritt) gerade $q^{2(n-(n+1)+1)}-1=0$ ist. Aus Lemma (3.7) bekommen wir

$$\begin{bmatrix} n_{m-1}-j \\ n_{m-1}-r+1\end{bmatrix}+q^{2(r-j)}\begin{bmatrix} n_{m-1}-j \\ n_{m-1}-r\end{bmatrix} = \begin{bmatrix} n_{m-1}-j+1 \\ n_{m-1}-r+1\end{bmatrix}$$

und erhalten damit

$$\sum_{j=0}^{r}(-1)^{r-j}q^{(r-j)(r-j-1)}\begin{bmatrix} n_{m-1}+1-s \\ j\end{bmatrix}q^{2j}c_{m-1}^j\begin{bmatrix} n_{m-1}-j+1 \\ n_{m-1}-r+1\end{bmatrix}.$$

Wir betrachten kurz, wie n_m und n_{m+2} bzw. c_m und c_{m+2} zusammenhängen. Nach Definition gilt

$$n_m = \left\lfloor \frac{m}{2}\right\rfloor \quad \text{und} \quad c_m = q^{m(m-1)/(2n)}.$$

Für gerades $m=2k$ haben wir

$$n_{2k} = \left\lfloor \frac{2k}{2}\right\rfloor = k$$

und

$$c_{2k} = q^{2k(2k-1)/(2k)} = q^{2k-1}.$$

Für ungerades $m = 2k+1$ haben wir

$$n_{2k+1} = \left\lfloor \frac{2k+1}{2} \right\rfloor = k$$

und

$$c_{2k+1} = q^{(2k+1)(2k+1-1)/(2k)} = q^{2k+1}.$$

Folglich

$$n_{m+2} = n_m + 1 \text{ und } c_{m+2} = q^2 c_m.$$

Dies liefert

$$\sum_{j=0}^{r} (-1)^{r-j} q^{(r-j)(r-j-1)} \begin{bmatrix} n_{m+1}-j \\ n_{m+1}-r \end{bmatrix} \begin{bmatrix} n_{m+1}-s \\ j \end{bmatrix} c_{m+1}^j = F_r^{(m+1)}(s)$$

nach Definition. Die Additionsformel

$$q^{2r} F_r^{(m-1)}(s-1) - q^{2(r-1)} F_{r-1}^{(m-1)}(s-1) = F_r^{(m+1)}(s) \qquad (*)$$

werden wir im Beweis weiterhin benötigen.
Nun nutzen wir Theorem (2.7) noch einmal für die Fälle $i = 2s-1$ und $\tau \in \{+1, -1\}$. Wir bekommen

$$\begin{aligned}
& 2Q_{2r,1}(i,\tau) + 2Q_{2r,-1}(i,\tau) + 2Q_{2r-1,1}(i,\tau) + 2Q_{2r-1,-1}(i,\tau) \\
= \quad & q^{2r} F_r^{(m-1)}(s-1) + \eta(-1)^r q^r F_r^{(m)}(s-1) \\
& + q^{2r} F_r^{(m-1)}(s-1) - \eta(-1)^r q^r F_r^{(m)}(s-1) \\
& - q^{2(r-1)} F_{r-1}^{(m-1)}(s-1) + \tau\eta(-1)^{s-1+r-1} q^{m-(s-1)+r-1-1} \gamma_q F_{r-1}^{(m-1)}(s-1) \\
& - q^{2(r-1)} F_{r-1}^{(m-1)}(s-1) - \tau\eta(-1)^{s-1+r-1} q^{m-(s-1)+r-1-1} \gamma_q F_{r-1}^{(m-1)}(s-1) \\
= \; & 2q^{2r} F_r^{(m-1)}(s-1) - 2q^{2(r-1)} F_{r-1}^{(m-1)}(s-1),
\end{aligned}$$

sodass wir als ursprüngliche Summe mit $(*)$ wieder

$$q^{2r} F_r^{(m-1)}(s-1) - q^{2(r-1)} F_{r-1}^{(m-1)}(s-1) = F_r^{(m+1)}(s)$$

erhalten. Damit haben wir gezeigt, dass in der Summe

$$\sum_{k,\epsilon} (Q_{2r,1}(k,\epsilon) + Q_{2r,-1}(k,\epsilon) + Q_{2r-1,1}(k,\epsilon) + Q_{2r-1,-1}(k,\epsilon)) a_{k,\epsilon}$$

der Vorfaktor der Zahlen $a_{2s,1}, a_{2s,-1}, a_{2s-1,1}$ und $a_{2s-1,1}$ für jedes s gleich ist, und zwar $F_r^{(m+1)}(s)$. Wir können diese also in der Summe zu A_s zusammenfassen und erhalten damit für jedes r die gewünschte Gleichheit

$$A'_r = \sum_{s=0}^{n} F_r^{(m+1)}(s) A_s.$$

Man beachte, dass die Formeln in Theorem (2.7) zunächst nur für $Q_{k,\epsilon}(i,\tau)$ mit $k,i \geq 1$ gelten. Man sieht aber sofort, dass sie auch im Fall $k=0$ richtig sind, denn dann ist

$$Q_{0,\epsilon}(i,\tau) = \frac{1+\epsilon}{2} \text{ für jedes i,}$$

also $Q_{0,1}(2s,\tau) = Q_{0,1}(2s-1,\tau) = 1 = F_0^{(m+1)}(s)$ wie gewünscht, sodass wir diesen Fall bei keiner der vier Gleichungen gesondert betrachten müssen. Eigenwerte der Form $Q_{k,\epsilon}(0,1)$ sind allerdings noch nicht durch diese Rechnung abgedeckt. Hier benötigt man explizite Darstellungen der Zahlen $Q_{k,\epsilon}(0,1) = v(k,\epsilon)$ (siehe dafür etwa Proposition 2.1 in [12]) und muss die entsprechende Summe der Valenzen dann mit Satz (4.2) und (4.3) zu $F_r^{(m+1)}(0)$ umformen. Wir werden den Spezialfall $i=0$ bei den vier Gleichungen aus Platzgründen nicht beweisen.
Nun betrachten wir die zweite Gleichung. Nach Definition haben wir

$$B'_r = a'_{2r,1} + a'_{2r,-1} + a'_{2r+1,1} + a'_{2r+1,-1},$$

sodass wir mit denselben Argumenten wie zuvor nun für alle i und τ die Summe

$$2Q_{2r,1}(i,\tau) + 2Q_{2r,-1}(i,\tau) + 2Q_{2r+1,1}(i,\tau) + 2Q_{2r+1,-1}(i,\tau)$$

ausrechnen müssen. Mit Theorem (2.7) erhalten wir für gerades $i = 2s \neq 0$ und $\tau \in \{+1,-1\}$

$$\begin{aligned}
& q^{2r}F_r^{(m-1)}(s-1) - \tau\eta(-1)^s q^{m-s+2r-2}F_{r-1}^{(m-2)}(s-1) + \eta(-1)^r q^r F_r^{(m)}(s) \\
&+ q^{2r}F_r^{(m-1)}(s-1) - \tau\eta(-1)^s q^{m-s+2r-2}F_{r-1}^{(m-2)}(s-1) - \eta(-1)^r q^r F_r^{(m)}(s) \\
&- q^{2r}F_r^{(m-1)}(s-1) + \tau\eta(-1)^s q^{m-s+2r}F_r^{(m-2)}(s-1) \\
&- q^{2r}F_r^{(m-1)}(s-1) + \tau\eta(-1)^s q^{m-s+2r}F_r^{(m-2)}(s-1) \\
= \quad & 2\tau\eta(-1)^s q^{m-s+2r}F_r^{(m-2)}(s-1) - 2\tau\eta(-1)^s q^{m-s+2r-2}F_{r-1}^{(m-2)}(s-1),
\end{aligned}$$

also mit $(*)$

$$q^m\tau\eta(-1)^s q^{-s}\left(q^{2r}F_r^{(m-2)}(s-1) - q^{2(r-1)}F_{r-1}^{(m-2)}(s-1)\right) = q^m\tau\eta(-1)^s q^{-s}F_r^{(m)}(s)$$

als ursprüngliche Summe. Für ungerades $i = 2s+1$ liefert Theorem (2.7)

$$\begin{aligned}
& q^{2r}F_r^{(m-1)}(s) + \eta(-1)^r q^r F_r^{(m)}(s) \\
&+ q^{2r}F_r^{(m-1)}(s) - \eta(-1)^r q^r F_r^{(m)}(s) \\
&- q^{2r}F_r^{(m-1)}(s) + \tau\eta(-1)^{s+r} q^{m-s+r-1}\gamma_q F_r^{(m-1)}(s) \\
&- q^{2r}F_r^{(m-1)}(s) - \tau\eta(-1)^{s+r} q^{m-s+r-1}\gamma_q F_r^{(m-1)}(s) \\
= \quad & 0.
\end{aligned}$$

Also ist der Vorfaktor von $a_{2s,1}$ gleich $q^m\eta(-1)^s q^{-s}F_r^{(m)}(s)$ und der von $a_{2s,-1}$ gleich $-q^m\eta(-1)^s q^{-s}F_r^{(m)}(s)$, für ungerade i ist der Vorfaktor von $a_{i,\tau}$ gleich 0. Nach Definition der Zahlen C_s können wir also nun für jedes r schreiben

$$B'_r = q^m \sum_{s=0}^{n} F_r^{(m)}(s) C_s,$$

damit ist die zweite Gleichung bewiesen.
Nun zeigen wir die Formel für die Zahlen C'_r. Nach Definition haben wir

$$C'_r = \eta(-1)^r q^{-r}(a'_{2r,1} - a'_{2r,-1}),$$

sodass wir dieses Mal

$$Q_{2r,1}(i,\tau) - Q_{2r,-1}(i,\tau)$$

betrachten. Theorem (2.7) liefert uns für gerades $i = 2s \neq 0$ und $\tau \in \{+1,-1\}$

$$\begin{aligned} &q^{2r}F_r^{(m-1)}(s-1) - \tau\eta(-1)^s q^{m-s+2r-2}F_{r-1}^{(m-2)}(s-1) + \eta(-1)^r q^r F_r^{(m)}(s) \\ -&\Big(q^{2r}F_r^{(m-1)}(s-1) - \tau\eta(-1)^s q^{m-s+2r-2}F_{r-1}^{(m-2)}(s-1) - \eta(-1)^r q^r F_r^{(m)}(s)\Big) \\ &= 2\eta(-1)^r q^r F_r^{(m)}(s), \end{aligned}$$

und somit ist $\eta(-1)^r q^r F_r^{(m)}(s)$ die Summe der beiden Eigenwerte. Wegen $\eta(-1) \in \{+1,-1\}$ ist $\eta(-1)^{2r} = 1$, sodass nach Multiplikation mit $\eta(-1)^r q^{-r}$ aus der Definition der C'_r lediglich $F_r^{(m)}(s)$ als Vorfaktor von $a_{2s,\tau}$ übrig bleibt. Dasselbe rechnen wir mit Theorem (2.7) nochmal für ungerades $i = 2s+1$ und $\tau \in \{+1,-1\}$ aus. Hier erhalten wir

$$\begin{aligned} &q^{2r}F_r^{(m-1)}(s) + \eta(-1)^r q^r F_r^{(m)}(s) \\ -&\Big(q^{2r}F_r^{(m-1)}(s) - \eta(-1)^r q^r F_r^{(m)}(s)\Big) \\ &= 2\eta(-1)^r q^r F_r^{(m)}(s), \end{aligned}$$

und damit mit denselben Argumenten $F_r^{(m)}(s)$ als Vorfaktor von $a_{2s+1,\tau}$. Also haben $a_{2s,1}, a_{2s,-1}, a_{2s+1,1}$ und $a_{2s+1,-1}$ für jedes s denselben Vorfaktor, sodass wir nach Definition der B_s schreiben können

$$C'_r = \sum_{s=0}^{n} F_r^{(m)}(s) B_s.$$

Nun bleibt noch eine Gleichheit zu zeigen. Die Zahlen D'_r sind definiert als

$$D'_r \coloneqq \eta(-1)^r q^{-r}(a'_{2r+1,1} - a'_{2r+1,-1}),$$

hier müssen wir also für alle Paare (i,τ) die Summe

$$Q_{2r+1,1}(i,\tau) - Q_{2r+1,-1}(i,\tau)$$

ausrechnen. Für gerades $i = 2s \neq 0$ und $\tau \in \{+1, -1\}$ liefert uns Theorem (2.7)

$$\begin{aligned} &- q^{2r} F_r^{(m-1)}(s-1) + \tau\eta(-1)^s q^{m-s+2r} F_r^{(m-2)}(s-1) \\ -&\Big(- q^{2r} F_r^{(m-1)}(s-1) + \tau\eta(-1)^s q^{m-s+2r} F_r^{(m-2)}(s-1)\Big) \\ &= 0 \end{aligned}$$

und für ungerades $i = 2s+1$ und $\tau \in \{+1, -1\}$ erhalten wir

$$\begin{aligned} &- q^{2r} F_r^{(m-1)}(s) + \tau\eta(-1)^{s+r} q^{m-s+r-1}\gamma_q F_r^{(m-1)}(s) \\ -&\Big(- q^{2r} F_r^{(m-1)}(s) - \tau\eta(-1)^{s+r} q^{m-s+r-1}\gamma_q F_r^{(m-1)}(s)\Big) \\ &= 2\tau\eta(-1)^{s+r} q^{m-s+r-1}\gamma_q F_r^{(m-1)}(s), \end{aligned}$$

also $\tau\eta(-1)^{s+r} q^{m-s+r-1}\gamma_q F_r^{(m-1)}(s)$ also Summe der beiden Eigenwerte. Nach Multiplikation mit $\eta(-1)^r q^{-r}$ aus der Definition der Zahlen D'_r bleibt noch

$$\tau q^{m-1}\eta(-1)^s q^{-s}\gamma_q F_r^{(m-1)}(s)$$

übrig. Also ist der Vorfaktor von $a_{2s+1,1}$ gleich $q^{m-1}\gamma_q\eta(-1)^s q^{-s} F_r^{(m-1)}(s)$ und der von $a_{2s+1,-1}$ gleich $-q^{m-1}\gamma_q\eta(-1)^s q^{-s} F_r^{(m-1)}(s)$. Da die Vorfaktoren der $a_{i,\tau}$ für gerades i gleich 0 sind, können wir nach Definition der D_s für jedes r schreiben

$$D'_r = q^{m-1}\gamma_q \sum_{s=0}^{n} F_r^{(m-1)}(s) D_s.$$

Damit ist das Theorem bewiesen. □

Damit haben wir Systeme von Zahlen gefunden, die dieselben Informationen wie die innere bzw. duale Verteilung enthalten. Mithilfe dieser beiden Systeme können wir nun Abschätzungen für die Kardinalität von d-Codes in $X(m, q)$ beweisen.

4 d-Codes in $X(m, q)$

In diesem Kapitel arbeiten wir Abschnitt 2 in Kapitel 3 in [12] aus. Dazu beweisen wir zunächst die dort gegebenen Rechenregeln und leiten anschließend eine Schranke für die Größe von d-Codes in $X(m, q)$ her. Zum Schluss geben wir einen Ausblick auf noch ungelöste Fragen und weitere Forschungsmöglichkeiten.

4.1 Vorbereitung der Beweise

Um die Sätze in diesem Kapitel zu beweisen, benötigen wir Eigenschaften des Gauß-Koeffizienten und der Zahlen $F_r^{(m)}(s)$. Ziel dieses Abschnittes ist der Beweis des folgenden Satzes:

4.1 Satz. [12, Gleichung (2.8)] *Für $j \in \{0, \dots, n\}$ gilt*

$$\sum_{r=0}^{j} \begin{bmatrix} n-r \\ n-j \end{bmatrix} F_r^{(m)}(s) = \begin{bmatrix} n-s \\ j \end{bmatrix} c^j.$$

Dabei ist wieder

$$n \coloneqq \left\lfloor \frac{m}{2} \right\rfloor \text{ und } c \coloneqq q^{m(m-1)/(2n)}.$$

Wir zeigen dazu zwei Hilfsaussagen, die am Ende von Kapitel 2 in [12] zu finden sind.

4.2 Satz. *Für $n \in \mathbb{N}$ und $a, b \in \mathbb{R}$ gilt*

$$\prod_{k=0}^{n-1} (a + q^{2k} b) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} q^{k(k-1)} a^{n-k} b^k.$$

Beweis. Wir schreiben

$$(a+b)(a+q^2b)(a+q^4b)\dots(a+q^{2(n-1)}b) = \sum_{k=0}^{n} f(n,k) a^{n-k} b^k$$

und erweitern um den nächsten Faktor

$$(a+b)(a+q^2b)(a+q^4b)\dots(a+q^{2(n-1)}b)(a+q^{2n}b) = \left(\sum_{k=0}^{n} f(n,k) a^k b^{n-k} \right) (a+q^{2n}b).$$

Der Koeffizient von $a^{n+1-r} b^r$ ist für $r \in \{0, \dots, n+1\}$ gegeben durch

$$f(n+1, r) = f(n, r) + q^{2n} f(n, r-1), \qquad (*)$$

beachte dabei $f(n,-1) = f(n,n+1) = 0$. Wir zeigen nun mit vollständiger Induktion nach n, dass für alle $r \leq n$ gilt

$$f(n,r) = \begin{bmatrix} n \\ r \end{bmatrix} q^{r(r-1)}.$$

Wir überprüfen zunächst den Fall $n = 1$:

$$\prod_{k=0}^{0}(a+q^{2k}b) = a+b = \begin{bmatrix} 1 \\ 0 \end{bmatrix} q^{0\cdot(-1)}a^{1-0}b^0 + \begin{bmatrix} 1 \\ 1 \end{bmatrix} q^{1\cdot 0}a^{1-1}b^1 = f(1,0)\cdot a + f(1,1)\cdot b.$$

Nun gelte

$$f(n,r) = \begin{bmatrix} n \\ r \end{bmatrix} q^{r(r-1)}$$

für ein festes $n \in \mathbb{N}$ und alle $r \leq n$. Mit der Rekursionsformel $(*)$ erhalten wir für ein beliebiges $r \in \{1,\dots,n\}$

$$\begin{aligned} &f(n+1,r) = f(n,r) + q^{2n}f(n,r-1) \\ =&\begin{bmatrix} n \\ r \end{bmatrix} q^{r(r-1)} + q^{2n}\begin{bmatrix} n \\ r-1 \end{bmatrix} q^{(r-1)(r-2)} \\ =& q^{r(r-1)}\left(\begin{bmatrix} n \\ r \end{bmatrix} + q^{2(n-(r-1))}\begin{bmatrix} n \\ r-1 \end{bmatrix}\right) \\ =& q^{r(r-1)}\begin{bmatrix} n+1 \\ r \end{bmatrix} \end{aligned}$$

nach Lemma (3.7). Für die Randfälle $r = 0$ und $r = n+1$ beachte man, dass ein Summand in der Rekursionsformel $(*)$ gleich 0 ist, und wir auch hier wegen

$$\begin{bmatrix} n \\ n \end{bmatrix} = \begin{bmatrix} n \\ 0 \end{bmatrix} = 1$$

das richtige Ergebnis erhalten. □

4.3 Satz. *Für $n,k,i \in \mathbb{N}_0$ gilt*

$$\begin{bmatrix} n \\ k \end{bmatrix}\begin{bmatrix} k \\ i \end{bmatrix} = \begin{bmatrix} n \\ i \end{bmatrix}\begin{bmatrix} n-i \\ n-k \end{bmatrix}.$$

Beweis. Ohne Beschränkung der Allgemeinheit sei $n \geq k \geq i$, sonst sind beide Seiten der Gleichung gleich 0. Wir benutzen lediglich Standardtechniken wie Indexverschiebung, Aufteilen eines Produktes in zwei Produkte und Umkehrung der Zählrichtung. Damit

erhalten wir

$$\begin{aligned}
\begin{bmatrix} n \\ k \end{bmatrix}\begin{bmatrix} k \\ i \end{bmatrix} &= \left(\prod_{r=1}^{k}\frac{q^{2(n-r+1)}-1}{q^{2r}-1}\right)\left(\prod_{r=1}^{i}\frac{q^{2(k-r+1)}-1}{q^{2r}-1}\right)\\
&= \left(\prod_{r=1}^{i}\frac{q^{2(n-r+1)}-1}{q^{2r}-1}\right)\left(\prod_{r=i+1}^{k}\frac{q^{2(n-r+1)}-1}{q^{2r}-1}\right)\left(\prod_{r=1}^{i}\frac{q^{2(k-r+1)}-1}{q^{2r}-1}\right)\\
&= \begin{bmatrix} n \\ i \end{bmatrix}\left(\prod_{r=1}^{k-i}\frac{q^{2(n-i-r+1)}-1}{q^{2(r+i)}-1}\right)\left(\prod_{r=1}^{k-i}\frac{q^{2(k-r+1)}-1}{q^{2r}-1}\right)\left(\prod_{r=k-i+1}^{i}\frac{q^{2(k-r+1)}-1}{q^{2r}-1}\right)\\
&= \begin{bmatrix} n \\ i \end{bmatrix}\left(\prod_{r=1}^{k-i}\frac{q^{2(n-i-r+1)}-1}{q^{2r}-1}\right)\left(\prod_{r=1}^{k-i}\frac{q^{2(k-r+1)}-1}{q^{2(r+i)}-1}\right)\left(\prod_{r=k-i+1}^{i}\frac{q^{2(k-r+1)}-1}{q^{2r}-1}\right)\\
&= \begin{bmatrix} n \\ i \end{bmatrix}\begin{bmatrix} n-i \\ k-i \end{bmatrix}\left(\prod_{r=1}^{k-i}\frac{q^{2(k-r+1)}-1}{q^{2(r+i)}-1}\right)\left(\prod_{r=k-i+1}^{i}\frac{q^{2(k-r+1)}-1}{q^{2r}-1}\right).
\end{aligned}$$

Nun zeigen wir noch, dass die hinteren beiden Produkte den Wert 1 haben. Dazu durchlaufen wir die Produkte im Nenner rückwärts und erhalten

$$\begin{aligned}
&\left(\prod_{r=1}^{k-i}\frac{q^{2(k-r+1)}-1}{q^{2((k-i-r+1)+i)}-1}\right)\left(\prod_{r=k-i+1}^{i}\frac{q^{2(k-r+1)}-1}{q^{2(i-r+k-i+1)}-1}\right)\\
&= \left(\prod_{r=1}^{k-i}\frac{q^{2(k-r+1)}-1}{q^{2(k-r+1)}-1}\right)\left(\prod_{r=k-i+1}^{i}\frac{q^{2(k-r+1)}-1}{q^{2(k-r+1)}-1}\right)\\
&= 1. \qquad \square
\end{aligned}$$

Nun können wir Satz (4.1) beweisen.

Beweis von (4.1). Zu zeigen ist

$$\sum_{r=0}^{j}\begin{bmatrix} n-r \\ n-j \end{bmatrix}F_r^{(m)}(s) = \begin{bmatrix} n-s \\ j \end{bmatrix}c^j$$

für $j \in \{0,\dots,n\}$. Nach Definition der Zahlen $F_r^{(m)}(s)$ gilt

$$\begin{aligned}
\sum_{r=0}^{j}\begin{bmatrix} n-r \\ n-j \end{bmatrix}F_r^{(m)}(s) &= \sum_{r=0}^{j}\begin{bmatrix} n-r \\ n-j \end{bmatrix}\sum_{i=0}^{r}(-1)^{r-i}q^{(r-i)(r-i-1)}\begin{bmatrix} n-i \\ n-r \end{bmatrix}\begin{bmatrix} n-s \\ i \end{bmatrix}c^i\\
&= \sum_{r=0}^{j}\sum_{i=0}^{r}(-1)^{r-i}q^{(r-i)(r-i-1)}\begin{bmatrix} n-r \\ n-j \end{bmatrix}\begin{bmatrix} n-i \\ n-r \end{bmatrix}\begin{bmatrix} n-s \\ i \end{bmatrix}c^i.
\end{aligned}$$

Die zweite Summe können wir auch bis j laufen lassen, da der zweite Gauß-Koeffizient nur für $i \le r$ ungleich 0 ist. Wegen $r \le j$ geht kein Summand verloren und alle hinzukommenden Terme sind gleich 0. Nun können wir die Summen vertauschen und die

andere Summe von i bis j laufen lassen (nur dann sind beide Gauß-Koeffizienten ungleich 0). Wir erhalten dann mit Satz (4.3)

$$\begin{aligned}
&\sum_{i=0}^{j}\sum_{r=i}^{j}(-1)^{r-i}q^{(r-i)(r-i-1)}\begin{bmatrix}n-r\\ n-j\end{bmatrix}\begin{bmatrix}n-i\\ n-r\end{bmatrix}\begin{bmatrix}n-s\\ i\end{bmatrix}c^i\\
&\sum_{i=0}^{j}\begin{bmatrix}n-s\\ i\end{bmatrix}c^i\sum_{r=i}^{j}(-1)^{r-i}q^{(r-i)(r-i-1)}\begin{bmatrix}n-i\\ n-j\end{bmatrix}\begin{bmatrix}j-i\\ r-i\end{bmatrix}\\
=&\sum_{i=0}^{j}\begin{bmatrix}n-s\\ i\end{bmatrix}c^i\begin{bmatrix}n-i\\ n-j\end{bmatrix}\sum_{r=0}^{j-i}(-1)^r q^{r(r-1)}\begin{bmatrix}j-i\\ r\end{bmatrix}.
\end{aligned}$$

Auf die innere Summe wenden wir nun Satz (4.2) mit $n=j-i, a=1$ und $b=-1$ an und erhalten

$$\sum_{i=0}^{j}\begin{bmatrix}n-s\\ i\end{bmatrix}c^i\begin{bmatrix}n-i\\ n-j\end{bmatrix}\prod_{r=0}^{j-i-1}(1-q^{2r}).$$

Wir sehen sofort, dass das Produkt für $j-i\geq 1$ gleich 0 ist, da dann der Faktor $1-q^{2\cdot 0}$ vorkommt. Also können wir $j-i\leq 0$ annehmen, d.h. $j\leq i$. Zusammen mit $i\leq j$ (da i von 0 bis j läuft) haben wir $i=j$ und in diesem Fall hat das Produkt den Wert 1. Wir können es also durch das Kronecker-Delta ersetzen und erhalten

$$\sum_{i=0}^{j}\begin{bmatrix}n-s\\ i\end{bmatrix}c^i\begin{bmatrix}n-i\\ n-j\end{bmatrix}\delta_{ij}=\begin{bmatrix}n-s\\ j\end{bmatrix}c^j\begin{bmatrix}n-j\\ n-j\end{bmatrix}=\begin{bmatrix}n-s\\ j\end{bmatrix}c^j$$

wie gewünscht. □

4.2 Schranken für d-Codes

Wir benutzen nun Satz (4.1), um eine Schranke für d-Codes herzuleiten. Dazu zeigen wir zwei Sätze, die wir schließlich zu einem Theorem zusammenfassen.

4.4 Satz. [12, Lemma 3.5] *Sei Y ein $(2d-1)$-Code in $X(m,q)$ für ein $d\in\mathbb{N}$. Dann gilt:*

$$|Y|\leq\begin{cases}q^{(m+1)(m/2-d+1)} & \text{für gerades } m\\ q^{m((m+1)/2-d+1)} & \text{für ungerades } m\end{cases}$$

Dabei gilt Gleichheit genau dann, wenn Y ein $(2t+2)$-Design mit $t=\left\lfloor\frac{m+1}{2}\right\rfloor-d$ ist.

Beweis. Sei $(a_{i,\tau})$ die innere Verteilung von Y und seien (A_s) und (A'_r) die den Verteilungen zugeordneten Zahlen aus (3.6). Außerdem sei

$$n:=\left\lfloor\frac{m+1}{2}\right\rfloor\ \text{ und }\ c:=q^{m(m+1)/(2n)}.$$

Aus Satz (4.1) mit $j = n-d+1$ und Satz (3.6) schließen wir

$$\sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} A'_r = \sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} \sum_{s=0}^{n} F_r^{(m+1)}(s) A_s$$
$$= \sum_{s=0}^{n} A_s \sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} F_r^{(m+1)}(s) = c^{n-d+1} \sum_{s=0}^{n} \begin{bmatrix} n-s \\ n-d+1 \end{bmatrix} A_s.$$

Da Y ein $(2d-1)$-Code ist, ist $a_{i,\tau} = 0$ für $0 < i < 2d-1$, und damit $A_s = a_{2s,1} + a_{2s,-1} + a_{2s-1,1} + a_{2s-1,-1} = 0$ für $0 < i < d$, d.h. die Summanden auf der rechten Seite für $s = 1, \ldots, d-1$ sind alle gleich 0. Mit Lemma (3.1) und Theorem (2.7) haben wir $A_0 = a_{0,1} = 1$ und $A'_0 = a'_{0,1} = \sum_{i,\tau} Q_{0,1}(i,\tau) a_{i,\tau} = \sum_{i,\tau} a_{i,\tau} = |Y|$. Wegen

$$\begin{bmatrix} n \\ k \end{bmatrix} = 0 \text{ für } n < k$$

sind alle Summanden für $s \geq d$ gleich 0, also ist auf der rechten Seite nur der Summand für $s = 0$ ungleich 0, sodass sich die Summe auf

$$\sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} A'_r = c^{n-d+1} \begin{bmatrix} n \\ n-d+1 \end{bmatrix}$$

reduziert. Der Term für $r = 0$ in der linken Summe ist

$$\begin{bmatrix} n \\ d-1 \end{bmatrix} A'_0 = \begin{bmatrix} n \\ d-1 \end{bmatrix} |Y| .$$

Bringen wir diesen auf die andere Seite, so erhalten wir mit Lemma (2.6)

$$\sum_{r=1}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} A'_r = \begin{bmatrix} n \\ d-1 \end{bmatrix} \left(c^{n-d+1} - |Y| \right) .$$

Da die linke Seite nach Satz (3.3) und der Definition der (A'_r) reell und nicht negativ ist, muss also

$$|Y| \leq c^{n-d+1}$$

gelten. Für gerades $m = 2k$ haben wir

$$n = \left\lfloor \frac{2k+1}{2} \right\rfloor = k \quad \text{und} \quad c = q^{2k(2k+1)/(2k)} = q^{2k+1} = q^{m+1}$$

und damit

$$|Y| \leq (q^{m+1})^{k-d+1} = q^{(m+1)(m/2-d+1)}.$$

Für ungerades $m = 2k-1$ haben wir

$$n = \left\lfloor \frac{2k-1+1}{2} \right\rfloor = k \text{ und } c = q^{(2k-1)(2k-1+1)/(2k)} = q^{2k-1} = q^m$$

und damit

$$|Y| \leq (q^m)^{k-d+1} = q^{m((m+1)/2-d+1)},$$

was zu zeigen war.
Gilt nun sogar Gleichheit, so muss die linke Seite der Gleichung gleich 0 sein. Da keiner der Gauß-Koeffizienten 0 ist, muss also

$$A'_1 = \ldots = A'_{n-d+1} = 0$$

gelten. Wieder mit Satz (3.3) und der Definition der (A'_r) folgt daraus, dass

$$a'_{1,1} = a'_{1,-1} = \ldots = a'_{2(n-d+1),1} = a'_{2(n-d+1),-1} = 0,$$

also ist Y ein $(2n-2d+2)$-Design mit $n = \left\lfloor \frac{m+1}{2} \right\rfloor$, etwas anders aufgeschrieben also ein $(2t+2)$-Design mit $t = \left\lfloor \frac{m+1}{2} \right\rfloor - d$. □

Insbesondere können $(2d-1)$-Codes in $X(m,q)$ konstruiert werden, die diese Schranke mit Gleichheit erfüllen, sie ist also optimal. Außerdem ist die innere Verteilung von Y im Fall, dass Gleichheit gilt, eindeutig bestimmt, siehe dazu Kapitel 4 in [12] und Theorem 3.9 in [12].
Die nächste Schranke, also Satz (4.7), gilt nicht für beliebige d-Codes in $X(m,q)$. Wir benötigen dafür folgenden Begriff:

Definition. Eine Teilmenge Y von $X(m,q)$ heißt *additiv*, wenn sie eine Untergruppe von $(X(m,q),+)$ ist.

Für die innere Verteilung eines additiven Codes gilt:

4.5 Lemma. [12] *Ist $Y \subseteq X(m,q)$ additiv, so gilt für alle i,τ*

$$a_{i,\tau} = |Y \cap X_{i,\tau}|,$$

wobei $X_{i,\tau}$ wieder die Menge aller symmetrischen Bilinearformen in $X(m,q)$ mit Rang i und Typ τ ist.

Beweis. Für i,τ ist

$$a_{i,\tau} = \frac{1}{|Y|} |(Y \times Y) \cap R_{i,\tau}|$$

und

$$R_{i,\tau} = \{(A,B) \in X(m,q) \mid A - B \in X_{i,\tau}\}.$$

Wir betrachten alle Paare der Form $(A,0)$ mit $A \in X_{i,\tau}$. Dies sind $|X_{i,\tau}|$ Stück und genau die Elemente in $R_{i,\tau}$, deren zweite Komponente gleich 0 ist. Nun können wir jedes Element $(A,B) \in (Y \times Y) \cap R_{i,\tau}$ schreiben als $(A-B,0)+(B,B)$ mit $A-B \in Y \cap X_{i,\tau}$ und

$B \in Y$ und diese Zerlegung ist offenbar eindeutig. Da Y additiv ist, liefert umgekehrt jede solche Zerlegung ein Element von $(Y \times Y) \cap R_{i,\tau}$. Also gilt

$$|(Y \times Y) \cap R_{i,\tau}| = |Y \cap X_{i,\tau}| \cdot |Y|.$$

und wir erhalten

$$a_{i,\tau} = \frac{1}{|Y|} |(Y \times Y) \cap R_{i,\tau}| = \frac{1}{|Y|} |Y \cap X_{i,\tau}| \cdot |Y| = |Y \cap X_{i,\tau}|. \qquad \square$$

Für einen additiven d-Code können wir mithilfe eines inneren Produktes $\langle \cdot, \cdot \rangle$ einen Dualraum definieren.

Definition. Sei $\chi : \mathbb{F}_q \to \mathbb{C}^*$ ein nicht trivialer Charakter. Dann definieren wir

$$\langle A, B \rangle \coloneqq \chi(tr(AB))$$

Offenbar ist $\langle \cdot, \cdot \rangle$ symmetrisch und linear in jeder Komponente. Für eine additive Teilmenge Y von $X(m,q)$ definieren wir den Dualraum $Y^\perp$ (bzgl. $\langle \cdot, \cdot \rangle$) als

$$Y^\perp \coloneqq \{B \in X(m,q) \mid \langle A, B \rangle = 1 \text{ für jedes } A \in Y\}.$$

Wir sehen sofort, dass $Y^\perp$ additiv ist. $\langle \cdot, \cdot \rangle$ ist zwar kein Skalarprodukt, aber die Definition ist analog zu der Definition des Orthogonalraums in euklidischen oder unitären Vektorräumen. Man beachte, dass das innere Produkt hier für ein Element des Dualraums immer den Wert 1 haben muss, da dies das Neutralelement im Zielbereich von $\langle \cdot, \cdot \rangle$ ist.

Wir werden folgende Eigenschaft des Dualraums ohne Beweis verwenden:

4.6 Satz. [5, Theorem 7] *Sei $Y \subseteq X(m,q)$ additiv und $Y^\perp$ der Dualraum von Y. Sei außerdem $(a'_{i,\tau})$ die duale Verteilung von Y und $(a^\perp_{i,\tau})$ die innere Verteilung von $Y^\perp$. Dann gilt für jedes i, τ*

$$|Y| a^\perp_{i,\tau} = a'_{i,\tau}.$$

Nun können wir die nächste Schranke herleiten:

4.7 Satz. [12, Lemma 3.6] *Sei Y ein additiver $2d$-Code in $X(m,q)$ für ein $d \in \mathbb{N}$. Dann gilt:*

$$|Y| \leq \begin{cases} q^{m(m/2-d+1)} & , \text{ falls } m \text{ gerade} \\ q^{(m+1)((m-1)/2-d+1)} & , \text{ falls } m \text{ ungerade} \end{cases}$$

Beweis. Sei $(a_{i,\tau})$ die innere Verteilung von Y und seien (B_s) und (C'_r) die den Verteilungen zugeordneten Zahlen aus (3.6). Außerdem sei

$$n \coloneqq \left\lfloor \frac{m}{2} \right\rfloor \text{ und } c \coloneqq q^{m(m-1)/(2n)}.$$

Aus Satz (3.6) und Satz (4.1) mit $j = n-d+1$ erhalten wir

$$\begin{aligned} q^{n-d+1} \sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} C'_r &= q^{n-d+1} \sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} \sum_{s=0}^{n} F_r^{(m)}(s) B_s \\ &= q^{n-d+1} \sum_{s=0}^{n} B_s \sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} F_r^{(m)}(s) \\ &= (cq)^{n-d+1} \sum_{s=0}^{n} \begin{bmatrix} n-s \\ n-d+1 \end{bmatrix} B_s. \end{aligned}$$

Da Y ein $(2d)$-Code ist, ist $a_{i,\tau} = 0$ für $0 < i < 2d$ und damit $B_s = a_{2s,1} + a_{2s,-1} + a_{2s+1,1} + a_{2s+1,-1} = 0$ für $0 < s < d$, d.h. die Summanden auf der rechten Seite für $s = 1, \ldots, d-1$ sind gleich 0. Aufgrund des Gauß-Koeffizienten werden wie im vorherigen Beweis alle Summanden für $s \geq d$ gleich 0, sodass in der Summe auf der rechten Seite nur der Term für $s = 0$ übrig bleibt. Mit $B_0 = a_{0,1} + a_{1,1} + a_{1,-1} = 1 + 0 + 0 = 1$ erhalten wir mit Lemma (2.6)

$$q^{n-d+1} \sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} C'_r = (cq)^{n-d+1} \begin{bmatrix} n \\ n-d+1 \end{bmatrix} = (cq)^{n-d+1} \begin{bmatrix} n \\ d-1 \end{bmatrix}.$$

Wir überlegen uns nun, dass die linke Seite der Gleichung durch $|Y|$ teilbar ist: Zunächst ist jeder Summand nach Definition der $C'_r = \eta(-1)^r q^{-r}(a'_{2r,1} - a'_{2r,-1})$ ein ganzzahliges Vielfaches von $(a'_{2r,1} - a'_{2r,-1})$, da $r \leq n-d+1$ und der Faktor q^{-r} somit von q^{n-d+1} ausgeglichen wird. Da wir nach Satz (4.6) wissen, dass die duale Verteilung $(a'_{i,\tau})$ von Y gleich dem $|Y|$-fachen der inneren Verteilung von $Y^\perp$ ist, und diese nach Satz (4.5) ganzzahlig ist, ist jeder Summand auf der linken Seite durch $|Y|$ teilbar. Folglich ist auch die rechte Seite durch $|Y|$ teilbar. Da Y eine Untergruppe von $X(m,q)$ ist, teilt $|Y|$ nach dem Satz von Lagrange die Gruppenordnung $|X(m,q)|$. Da $X(m,q)$ ein Vektorraum über $\mathbb{F}_q$ ist, ist $|X(m,q)| = q^k$ für ein $k \in \mathbb{N}_0$, sodass auch $|Y|$ von der Form q^l für ein $l \in \mathbb{N}_0$ sein muss.
Sei nun p die Primzahl, die q teilt. Dann teilt p natürlich auch $|Y|$. Da $\begin{bmatrix} n \\ d-1 \end{bmatrix}$ nicht durch p teilbar ist (Zähler und Nenner aller Brüche in der Definition sind ungleich 0 modulo p), muss $|Y|$ also $(cq)^{n-d+1}$ teilen, und wir erhalten

$$|Y| \leq (cq)^{n-d+1}.$$

Wir formen diesen Ausdruck nun noch wie im Beweis von Satz (4.4) in die gewünschte Form um. Zunächst sei $m = 2k$ gerade. Dann haben wir

$$n = \left\lfloor \frac{2k}{2} \right\rfloor = k \text{ und } c = q^{2k(2k-1)/(2k)} = q^{2k-1},$$

also

$$|Y| \leq (cq)^{n-d+1} = (q^{2k-1}q)^{k-d+1} = q^{m(m/2-d+1)}.$$

Nun sei $m = 2k+1$ ungerade. Dann ist

$$n = \left\lfloor \frac{2k+1}{2} \right\rfloor = k \quad \text{und} \quad c = q^{(2k+1)(2k+1-1)/(2k)} = q^{2k+1}$$

und wir erhalten

$$|Y| \leq (cq)^{n-d+1} = (q^{2k+1}q)^{k-d+1} = q^{(m+1)((m-1)/2-d+1)}. \qquad \square$$

Das folgende Theorem liefert eine optimale Schranke für beliebige, additive d-Codes in $X(m,q)$:

4.8 Theorem. [12, Theorem 3.3] *Sei Y ein additiver d-Code in $X(m,q)$ für ein $d \in \mathbb{N}$. Dann gilt:*

$$|Y| \leq \begin{cases} q^{m(m-d+2)/2} & \textit{falls } m \text{ - } d \textit{ gerade} \\ q^{(m+1)(m-d+1)/2} & \textit{falls } m \text{ - } d \textit{ ungerade} \end{cases}$$

Beweis. Hier müssen wir nur noch die Sätze (4.4) und (4.7) zusammensetzen. Wir betrachten zunächst den Fall, dass $m-d$ gerade ist. Sind m und $d = 2e$ beide gerade, so liefert Satz (4.7)

$$|Y| \leq q^{m(m/2-e+1)} = q^{m(m-2e+2)/2} = q^{m(m-d+2)/2}.$$

Sind m und $d = 2e-1$ beide ungerade, so erhalten wir mit Satz (4.4)

$$|Y| \leq q^{m((m+1)/2-e+1)} = q^{m(m+1-2e+2)/2} = q^{m(m-d+2)/2}.$$

und die Schranke ist für diesen Fall gezeigt.
Sei nun $m-d$ ungerade. Ist dabei m gerade und $d = 2e-1$ ungerade, so liefert Satz (4.4)

$$|Y| \leq q^{(m+1)(m/2-e+1)} = q^{(m+1)(m-2e+2)/2} = q^{(m+1)(m-d+1)/2}.$$

Ist m ungerade und $d = 2e$ gerade, so erhalten wir mit Satz (4.7)

$$|Y| \leq q^{(m+1)((m-1)/2-e+1)} = q^{(m+1)(m-1-2e+2)/2} = q^{(m+1)(m-d+1)/2}.$$

Damit ist das Theorem für alle m und d bewiesen. $\square$

Konstruktionen von additiven d-Codes in $X(m,q)$, für die in Theorem (4.8) Gleichheit gilt, findet man in Kapitel 4 in [12].

4.3 Ausblick auf weitere Forschung

Wie wir im obigen Abschnitt gesehen haben, haben d-Codes mit ungeradem d schöne und bereits gut untersuchte Eigenschaften: Die Schranke hängt nicht davon ab, ob der Code additiv ist oder nicht, und bei Gleichheit ist die innere Verteilung des Codes eindeutig bestimmt. Über d-Codes mit geradem d ist dagegen weniger bekannt. Satz (4.7) gilt

(zumindest mit dem angegebenen Beweis) nur für additive Codes und bei Gleichheit ist die innere Verteilung des Codes im Allgemeinen nicht eindeutig bestimmt. Siehe etwa Tabelle 1 in [12] für die vier verschiedenen möglichen inneren Verteilungen eines 2-Codes in $X(4,3)$. Dort wurden mit einem Computer alle möglichen Verteilungen berechnet.
Natürlich kann man für einen $(2d)$-Code auch Satz (4.4) benutzen, indem man ihn als $(2d-1)$-Code betrachtet. Die so erhaltene Schranke lässt sich aber noch etwas verbessern.

4.9 Theorem. [12, Proposition 3.7] *Sei Y ein $(2d)$-Code in $X(m,q)$. Dann gilt:*

$$|Y| \leq \begin{cases} q^{(m+1)(m/2-d+1)} \dfrac{1+q^{-m+2d-1}}{q+1} & \text{für gerades } m \\ q^{m((m+1)/2-d+1)} \dfrac{1+q^{-m+1}}{q+1} & \text{für ungerades } m \end{cases}$$

Beweis. Sei wieder $(a_{i,\tau})$ die innere Verteilung von Y und $(A_s), (B_s), (C_s)$ sowie $(A'_r), (B'_r), (C'_r)$ die den Verteilungen zugeordneten Zahlen aus (3.6).
Zunächst sei $m = 2n$ gerade. Wir betrachten

$$\sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} (A'_r + qC'_r)$$

und erhalten mit Satz (3.6) und Satz (4.1) daraus (man beachte, dass wir (4.1) mit demselben n aber zwei verschiedenen Zahlen c benutzen, da wir einmal $F_r^{(m+1)}(s)$ und einmal $F_r^{(m)}(s)$ in der Summe stehen haben)

$$\begin{aligned} &\sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} \left(\sum_{s=0}^{n} F_r^{(m+1)}(s) A_s + q \sum_{s=0}^{n} F_r^{(m)}(s) B_s \right) \\ =& \sum_{s=0}^{n} \left(A_s \sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} F_r^{(m+1)}(s) + qB_s \sum_{r=0}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} F_r^{(m)}(s) \right) \\ =& \sum_{s=0}^{n} \begin{bmatrix} n-s \\ n-d+1 \end{bmatrix} \left(A_s \left(q^{(m+1)m/(2n)}\right)^{n-d+1} + qB_s \left(q^{m(m-1)/(2n)}\right)^{n-d+1} \right) \\ =& \, q^{(m-1)(n-d+1)} \sum_{s=0}^{n} \begin{bmatrix} n-s \\ n-d+1 \end{bmatrix} \left(q^{2(n-d+1)} A_s + qB_s \right). \end{aligned}$$

Da Y ein $(2d)$-Code ist, haben wir $a_{i,\tau} = 0$ für $0 < i < 2d$ und $\tau \in \{+1, -1\}$, und damit $A_0 = B_0 = a_0 = 1$ sowie $A_s = a_{2s,1} + a_{2s,-1} + a_{2s-1,1} + a_{2s-1,-1} = 0$ und $B_s = a_{2s,1} + a_{2s,-1} + a_{2s+1,1} + a_{2s+1,-1} = 0$ für $0 < s < d$. Für $s \geq d$ sind die Gauß-Koeffizienten gleich 0, sodass wieder nur der erste Term der Summe ungleich 0 ist. Bringen wir nun den Term für $r = 0$ in der ursprünglichen Summe auf die rechte Seite, so erhalten wir wieder mit $A_0 = C_0 = a'_{0,1} = |Y|$

$$\sum_{r=1}^{n-d+1} \begin{bmatrix} n-r \\ d-1 \end{bmatrix} (A'_r + qC'_r) = \begin{bmatrix} n \\ d-1 \end{bmatrix} \left(q^{(m-1)(n-d+1)} \left(q^{2(n-d+1)} + q \right) - (q+1)|Y| \right).$$

Da die linke Seite nach Satz (3.3) nicht negativ ist, erhalten wir

$$\begin{aligned}|Y| &\leq \frac{q^{(m-1)(n-d+1)}\left(q^{2(n-d+1)}+q\right)}{q+1} = \frac{q^{(m+1)(n-d+1)}\left(1+q^{-2(n-d+1)+1}\right)}{q+1} \\ &= q^{(m+1)(m/2-d+1)}\frac{1+q^{-m+2d-1}}{q+1}.\end{aligned}$$

Sei nun $m = 2n+1$ ungerade. Hier betrachten wir

$$\sum_{r=0}^{n-d+1}\begin{bmatrix}n-r\\d-1\end{bmatrix}(B'_r + qC'_r)$$

und erhalten mit Satz (3.6) und Satz (4.1) daraus

$$\begin{aligned}&\sum_{r=0}^{n-d+1}\begin{bmatrix}n-r\\d-1\end{bmatrix}\left(q^m\sum_{s=0}^{n}F_r^{(m)}(s)C_s + q\sum_{s=0}^{n}F_r^{(m)}(s)B_s\right) \\ =&\sum_{s=0}^{n}\left(q^mC_s\sum_{r=0}^{n-d+1}\begin{bmatrix}n-r\\d-1\end{bmatrix}F_r^{(m)}(s) + qB_s\sum_{r=0}^{n-d+1}\begin{bmatrix}n-r\\d-1\end{bmatrix}F_r^{(m)}(s)\right) \\ =&\sum_{s=0}^{n}\begin{bmatrix}n-s\\n-d+1\end{bmatrix}\left(q^mC_s\left(q^{m(m-1)/(2n)}\right)^{n-d+1} + qB_s\left(q^{m(m-1)/(2n)}\right)^{n-d+1}\right) \\ =&q^{m(n-d+1)}\sum_{s=0}^{n}\begin{bmatrix}n-s\\n-d+1\end{bmatrix}\left(q^mC_s+qB_s\right).\end{aligned}$$

Genau wie oben haben wir $B_0 = C_0 = a_{0,1} = 1$ sowie $B_s = a_{2s,1} + a_{2s,-1} + a_{2s+1,1} + a_{2s+1,-1} = 0$ und $C_s = \eta(-1)^s q^{-s}(a_{2s,1} - a_{2s,-1}) = 0$ für $0 < s < d$, da Y ein $(2d)$-Code ist. Also ist wieder nur der erste Term der Summe ungleich 0. Bringen wir nun den Term für $r = 0$ in der ursprünglichen Summe auf die rechte Seite, so erhalten wir mit $C_0 = a'_{0,1} = |Y|$ und $B_0 = a'0, 1 + a'_{1,1} + a'_{1,-1} = |Y| + a'_{1,1} + a'_{1,-1}$ schließlich

$$\begin{aligned}&\begin{bmatrix}n\\d-1\end{bmatrix}(a'_{1,1}+a'_{1,-1}) + \sum_{r=1}^{n-d+1}\begin{bmatrix}n-r\\d-1\end{bmatrix}(B'_r+qC'_r) \\ =&\begin{bmatrix}n\\d-1\end{bmatrix}\left(q^{m(n-d+1)}\left(q^m+q\right)-(q+1)|Y|\right).\end{aligned}$$

Da die linke Seite nach Satz (3.3) nicht negativ ist, erhalten wir

$$\begin{aligned}|Y| &\leq \frac{q^{m(n-d+1)}(q^m+q)}{q+1} = q^{m(n-d+1)}\frac{q^m+q^mq^{-m}q}{q+1} \\ &= q^{m(n-d+2)}\frac{1+q^{-m+1}}{q+1} = q^{m((m+1)/2-d+1)}\frac{1+q^{-m+1}}{q+1}.\end{aligned}$$

□

Mit Theorem (4.9) haben wir eine Schranke für beliebige $(2d)$-Codes in $X(m,q)$ gefunden. Allerdings ist (im Gegensatz zu Satz (4.4)) nicht klar, ob diese Schranke optimal ist, d.h. ob für jede Wahl der Parameter m und q auch $(2d)$-Codes existieren, die die Schranke mit Gleichheit erfüllen.
Die Eigenschaften $a_{i,\tau}, a'_{i,\tau} \geq 0$ für alle i, τ machen es möglich, das Abschätzen von Größen von d-Codes als lineares Programm zu betrachten. Denn nach Lemma (3.1) haben wir

$$|Y| = \sum_{i,\tau} a_{i,\tau}$$

und können damit das lineare Programm

$$\begin{array}{lll} max & |Y| = \sum_{i,\tau} a_{i,\tau} & \\ s.t. & a_{i,\tau} & \geq 0 \\ & a'_{i,\tau} = \sum_{k,\epsilon} Q_{i,\tau}(k,\epsilon) a_{k,\epsilon} & \geq 0 \\ & a_{1,\pm 1} & = 0 \\ & \vdots & \\ & a_{d-1,\pm 1} & = 0 \end{array}$$

betrachten. Da jeder d-Code diese (Un-)Gleichungen erfüllen muss, kann die Größe des größtmöglichen d-Codes in $X(m,q)$ nicht größer sein, als der Maximalwert des linearen Programms. Es ist aber theoretisch möglich, dass das Optimum des linearen Programmes größer ist, als die Kardinalität des größten d-Codes, da nicht jede beliebige Folge von Zahlen $(a_{i,\tau})$ zu einem d-Code gehört (zum Beispiel könnte die Summe aller Zahlen nicht ganzzahlig sein). Es gibt aber Hinweise darauf, dass Satz (4.9) die optimale Lösung des linearen Programms liefert. Schmidt hat dies mit dem Simplex-Algorithmus für mehrere kleine Werte von m und q überprüft. Dies ist allerdings nicht bewiesen und bedarf weiterer Nachforschung.

5 Zusammenfassung und Fazit

Diese Arbeit soll in die Theorie der Assoziationsschemata einführen und diese am Beispiel des Assoziationsschemas der symmetrischen Bilinearformen über $\mathbb{F}_q$ mit der Codierungstheorie verbinden. Nachdem wir die Grundlagen der Theorie gegeben und an einigen Beispielen verdeutlicht haben, haben wir dem Vektorraum der symmetrischen Bilinearformen $X(m, q)$ die Struktur eines Assoziationsschemas gegeben. Anschließend sind wir näher auf die Struktur von Teilmengen eines Schemas eingegangen und haben Bezüge zur klassischen Codierungstheorie hergestellt. Zum Schluss haben wir Codes und Designs in $X(m, q)$ untersucht und konnten optimale Schranken für additive d-Codes finden. Im nicht additiven Fall weiß man nur über d-Codes mit ungeradem d Genaueres. Dagegen sind d-Codes mit geraden d noch ziemlich mysteriös, da nicht klar ist, ob die Schranke, die wir für additive Codes bewiesen haben, auch für nicht additive Codes gilt, und ob die anschließend bewiesene Schranke die optimale Schranke für d-Codes mit geradem d ist. Hier besteht weiterer Forschungsbedarf.

Literaturverzeichnis

[1] Albrecht Beutelspacher. *Lineare Algebra*. Springer, 2014.

[2] Raj Chandra Bose und K. R. Nair. "Partially Balanced Incomplete Block Designs". In: *Sankhya: The Indian Journal of Statistics* (1939).

[3] Raj Chandra Bose und T. Shimamoto. "Classification and Analysis of Partially Balanced Incomplete Block Designs with Two Associate Classes". In: *Journal of the American Statistical Association* (1952), S. 151–184.

[4] Philippe Delsarte. "An algebraic approach to the association schemes of coding theory". In: *Philips Research Reports Supplements no. 10* (1973).

[5] Philippe Delsarte und Vladimir I. Levenshtein. "Association schemes and coding theory". In: *IEEE Transactions on Information Theory* 44 (1998).

[6] Chris Godsil. *Association Schemes*. University of Waterloo. 2010.

[7] Yuanji Huo und Zhexian Wan. "Non-symmetric association schemes of symmetric matrices". In: *Acta Mathematicae Applicatae Sinica* (1993).

[8] Tsit-Yuen Lam. *Introduction to Quadratic Forms over Fields*. American Mathematical Society, 2005.

[9] Rudolf Lidl und Harald Niederreiter. *Finite Fields*. Bd. 20. Cambridge University Press, 1997.

[10] Florence Jessie MacWilliams und Neil James Alexander Sloane. *The Theory of Error-Correcting Codes*. Bd. 16. North-Holland Publishing Company, 1977.

[11] Morris Newman. "Two classical theorems on commuting matrices". In: *Journal of research of the National Bureau of Standards and Technology* (1967).

[12] Kai-Uwe Schmidt. "Symmetric bilinear forms over finite fields with applications to coding theory". In: *Journal of Algebraic Combinatorics* (2015).