Inauguraldissertation
zur
Erlangung der Doktorwürde
der
Naturwissenschaftlich-Mathematischen Gesamtfakultät
der
Ruprecht-Karls-Universität Heidelberg

vorgelegt von
Diplommathematiker Yves Edel
aus Ludwigshafen
26.11.1996

Eine Verallgemeinerung von BCH-Codes

Korrigierte Version

Gutachter: Dr. Jürgen Bierbrauer
Prof. Albrecht Brandis

Einleitung

Dem Leser, der nicht in der Codierungstheorie bewandert ist, wird zum besseren Verständnis empfohlen, erst Abschnitte 1.1 und 1.4 zu lesen.

In der Codierungstheorie ist es eine bekannte Tatsache, daß die Teilkörper-Teilcodes der Reed-Solomon-Codes die primitiven BCH-Codes sind. Die Codes, mit denen wir uns in dieser Arbeit beschäftigen werden, könnte man als Untervektorraum-Teilcodes der Reed-Solomon-Codes und allgemeiner BCH-Codes bezeichnen. Sie bestehen aus allen Worten des Reed-Solomon-Codes bzw. des BCH-Codes, deren sämtliche Einträge in einem Untervektorraum des Alphabets liegen. Diese Codes sind im allgemeinen nicht mehr linear, haben aber vieles mit den BCH-Codes gemeinsam. Die allgemeinen BCH-Codes sind als Spezialfälle zu erhalten.

Der Ausgangspunkt dieser Dissertation war J. Bierbrauers Arbeit [3] über die Konstruktion einer Klasse orthogonaler Arrays. Es blieb das offene Problem, die Dimension dieser Strukturen zu bestimmen. Als wir erkannten, daß im linearen Fall die dualen Codes, die erweiterten, primitiven BCH-Codes sind, also eine alte und eigentlich gut erforschte Klasse von Codes, waren glücklicherweise schon so viele neue Ergebnisse vorhanden, daß wir nicht an diesem Punkt die Arbeit an diesen Strukturen einstellten. Im weiteren Verlauf konnte der Autor dieses Konzept soweit verallgemeinern, daß man im linearen Fall die allgemeinen BCH-Codes erhält. Im Fall der nichtlinearen orthogonalen Arrays, der sich bei diesem Ansatz geradezu aufdrängt, bekommt man durch eine geeignete Verallgemeinerung der Dualität eine den BCH-Codes verwandte Klasse additiver Codes. Das Hauptproblem, die Dimensionsbestimmung all dieser Strukturen, konnte vollständig durchgeführt werden.

Für den Spezialfall der BCH-Codes, bekommt man bei diesem Zugang eine sehr einfache Methode der Dimensionsbestimmung. Etwas Vergleichbares hat der Autor in der Literatur nicht gefunden, obwohl rückblickend betrachtet alle benötigten Komponenten vorhanden waren und man sie nur hätte zusammenzusetzen müssen. Der hier beschrittene Weg der Dimensionsbestimmung wurde angeregt durch Rédeis Satz 3 [25], der die Lösung im Fall der primitiven narrow sense BCH-Codes liefert. Allerdings hat Rédei diese Anwendung seiner Theorie nicht im Auge.

In Abschnitt 1 werden die verwendeten Ergebnisse der Codierungstheorie zitiert. Es werden nur dann die Beweise mitgeliefert, wenn es sich um Verallgemeinerungen zur Standardliteratur (z.B. [22, 24]) handelt. Dies bedeutet oft nur, daß man den q-ären Fall betrachtet, da in der Literatur meist nur der binäre Fall behandelt wird. Desweiteren bekommt man die wichtigsten Ergebnisse auch durch Spezialisierung der Sätze in Abschnitt 2. In Abschnitt 1.3 bekommen wir aus der bis dahin entwickelten Theorie eine rekursive Code-Konstruktion, die neu zu sein scheint, die mit der weiteren Theorie aber nichts unmittelbar zu tun hat.

In Abschnitt 2 werden wir sehen, wie wir im „nichtlinearen“ Fall aus den orthogonalen Arrays einen Code als duale Struktur erhalten, sowie die wichtigsten Eigenschaften aus dem linearen Fall übertragen. Delsarte [13] hat das meiste davon für additive Codes schon getan. Wir werden uns hier aber stärker am linearen Fall orientieren. Sodann werden wir nun endlich zum Kern dieser Arbeit kommen. Wir führen unsere Verallgemeinerung der BCH-Codes ein und entwickeln deren Theorie. Der letzte Unterabschnitt beschäftigt sich dann mit der Dimensionsbestimmung dieser Codes.

Die nächsten vier Abschnitte sind eine Anwendung der erarbeiteten Theorie. Wir benutzen die einfachen rekursiven Methoden aus Abschnitt 1, sowie Weiterentwicklungen derselben, um aus unseren Codes Verbesserungen in A. Brouwers Datenbank binärer, ternärer und quaternärer linearer Codes [8] zu erhalten. Dabei sind die verwendeten Ausgangscodes in Abschnitt 3 und 5 die gewöhnlichen BCH-Codes. Daß man dabei trotzdem noch neue Codes findet, ist ein Indiz dafür, daß der hier gewählte Zugang zu den BCH-Codes deren Verständnis förderlich ist. Angesichts der bei den komplexeren Konstruktionen vielen freien Parameter, wurde die Suche nach Parametern, die zu einem neuen Code führen, mit einem einfachen Computerprogramm durchgeführt. Jedes einzelne Ergebnis läßt sich aber schnell und leicht von Hand durch die vorher entwickelte Theorie überprüfen. Einzig die überraschend große Zahl der neuen Codes gestaltet dies etwas langwierig.

In den Anhängen befinden sich die Codes, die man aus Abschnitt 1.3 bekommt, sowie eine geordnetes Verzeichnis aller gefundenen linearen Codes.

A. Brouwers Datenbank binärer, ternärer und quaternärer linearer Codes [8] befindet sich in elektronischer Form im *world wide web*. Sie wird fortlaufend ergänzt und so kann es kommen, daß Codes, die hier als neu bezeichnet werden, zwischenzeitlich bekannt sind. Die letzte in gedruckter Form veröffentlichte Version eines Teils der binären Datenbank [9] ist mittlerweile schon etwas veraltet. Codes, die die in der Datenbank angegebene obere Schranke für die Minimaldistanz d erreichen, nennen wir optimal. Alle in dieser Arbeit verwendeten Codes, die sich nicht unmittelbar aus den hier konstruierten Codes ableiten lassen, finden sich in A. Brouwers Datenbank [8]. Auszüge der Dissertation sind bereits als Manuskript erschienen bzw. zur Veröffentlichung eingereicht [4, 5, 16, 18, 17] und auch teilweise schon in die Datenbank eingegangen.

Inhaltsverzeichnis

1 Einführung in die Codierungstheorie

1.1 Grundlagen

Sei V, $|V| = v$, eine Menge genannt das *Alphabet*. Elemente in V^n nennen wir *Worte* der Länge n.

Definition 1.1 *Für zwei Elemente* $\mathbf{a}, \mathbf{b} \in V^n$ *ist die* Hammingdistanz $\mathrm{d}(\mathbf{a}, \mathbf{b})$ *definiert als:* $\mathrm{d}(\mathbf{a}, \mathbf{b}) := |\{i \,|a_i \neq b_i, 1 \leq i \leq n\}|$.
Ist V *eine Gruppe mit neutralem Element* 0*, so sei das* Gewicht $\mathrm{wt}(\mathbf{a})$ *als:* $\mathrm{wt}(\mathbf{a}) := \mathrm{d}(\mathbf{a}, \mathbf{0}) = |\{i \,|a_i \neq 0, 1 \leq i \leq n\}|$ *definiert.*

Definition 1.2 *Eine Teilmenge* $\mathcal{C} \subset V^n$, $|V| = v$, *heißt ein* (Block-)Code. *Gilt für alle* $\mathbf{a} \neq \mathbf{b} \in \mathcal{C}$, $d \leq \mathrm{d}(\mathbf{a}, \mathbf{b})$*, so nennt man* $\mathcal{C}$ *einen* v*-ären Code der* Länge n*,* Distanz d *und mit* $K = |\mathcal{C}|$ *Codeworten, kurz einen* v*-ären* $[n, K, d]$*. Die maximale Distanz* d*, so daß* $\mathcal{C}$ *ein* $[n, K, d]$ *ist, heißt die* Minimaldistanz $d_{\mathcal{C}}$ *von* $\mathcal{C}$*.*

Wenn man sich bei Teilmengen von V^n nicht für die Distanz, sondern für eine andere Eigenschaft, die Stärke, interessiert, so nennt man die Teilmengen von V^n auch orthogonale Arrays. Da sich die Theorie für die beiden Betrachtungsweisen zuerst unabhängig entwickelt hat, sind die Standardbezeichnungen leider nicht allzu kompatibel. Da es sich bei Distanz und Stärke nur um zwei verschiedene Eigenschaften einer Teilmenge von V^n handelt, hat natürlich jeder Code auch eine Stärke und jedes orthogonale Array auch eine Distanz. Wie wir später sehen werden, sind Distanz und Stärke in einem gewissen Sinne dual. Wir werden deshalb im folgenden der Einfachheit halber nur von Codes, mit eventuell einer gewissen Stärke, sprechen, wenn wir die allgemeine Situation im Auge haben und nur dann den Begriff orthogonales Array verwenden, wenn wir uns nur für die Stärke interessieren.

Definition 1.3 *Eine Teilmenge* $\mathcal{C} \subset V^n$, $|V| = v$, *heißt ein* orthogonales Array *der* Länge n*,* Stärke t *und* Vielfachheit λ*, kurz ein* $OA_\lambda(t, n, v)$*, falls es zu jedem Element* $\mathbf{x} \in V^t$ *und zu jeder* t*-Teilmenge* $I \subset \{1, \ldots, n\}$ *von Indizes genau* λ *verschiedene Elemente* $\mathbf{a} = (a_i) \in \mathcal{C}$ *gibt mit* $(a_i \,|i \in I) = \mathbf{x}$*. Man sagt* $\mathcal{C}$ *ist ein* $OA(t, n, v)$*, wenn man nur ausdrücken will, daß es eine Konstante* λ *gibt, so daß* $\mathcal{C}$ *ein* $OA_\lambda(t, n, v)$ *ist, man aber nicht an dem expliziten Wert von* λ *interessiert ist.*

Sei q, im weiteren Verlauf der Arbeit, immer eine Primzahlpotenz und $\mathbb{F}_q$ der Körper mit q Elementen.

Ist das Alphabet V eine Gruppe und ist die Summe zweier Codeworte von $\mathcal{C}$ wieder ein Codewort von $\mathcal{C}$, so spricht man von einem *additiven Code* bzw. *additiven OA*. Ist das Alphabet $V = \mathbb{F}_q$ und $\mathcal{C}$ ein $\mathbb{F}_q$-Vektorraum, so spricht man von einem *linearen Code* bzw. *linearen OA*. Ist k die Dimension von $\mathcal{C}$ als $\mathbb{F}_q$-Vektorraum, so nennt man $\mathcal{C}$ einen *k-dimensionalen Code* bzw. *OA*. Für lineare Codes der Länge n, Dimension k und Distanz d ist die Kurzform $[n, k, d]$ üblich, wobei das kleingeschriebene k helfen soll, Verwechslungen mit der Anzahl der Codeworte K im nichtlinearen Fall zu vermeiden.

Da bei einem linearen Code $\mathcal{C}$ die Differenz zweier Codeworte wieder ein Codewort ist, ist die Minimaldistanz von $\mathcal{C}$ gleich dem Minimalgewicht eines Codewortes ungleich Null, denn es gilt offenbar $\mathrm{d}(\mathbf{a}, \mathbf{b}) = \mathrm{d}(\mathbf{a} - \mathbf{b}, \mathbf{0}) = \mathrm{wt}(\mathbf{a} - \mathbf{b})$. Als Untervektorraum hat ein linearer Code $\mathcal{C}$ eine Basis $\mathbf{c}_1, \ldots, \mathbf{c}_k \in V^n$. Es ist üblich, die Basisvektoren als Zeilenvektoren zu schreiben. Eine $k \times n$ Matrix der Basisvektoren heißt eine *Erzeugermatrix* von $\mathcal{C}$.

Bemerkung 1.4 *Ein lineares orthogonales Array $\mathcal{C}$ hat Stärke t genau dann, wenn je beliebige t Spalten der Erzeugermatrix linear unabhängig sind.*

Beweis: Seien ObdA die ersten t Spalten der Erzeugermatrix linear abhängig. Sei M die Erzeugermatrix eingeschränkt auf die ersten t Spalten, so hat M nicht maximalen Rang. Somit kommt nicht jedes t-Tupel im Erzeugnis der Zeilen von M vor. Umgekehrt: sei M die Einschränkung auf t Spalten, diese sind nach Voraussetzung linear unabhängig, damit hat M maximalen Rang, also kommt jedes t-Tupel $\lambda = q^{k-t}$ mal im Erzeugnis der Zeilen von M vor, wobei k die Dimension der Erzeugermatrix des OA ist ■

Definition 1.5 *Sei $V = \mathbb{F}_q$, $\mathcal{C} \in V^n$ und $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i$ das Standardskalarprodukt auf $\mathbb{F}_q^n$. Dann heißt $\mathcal{C}^\perp := \{\mathbf{c}' \in \mathbb{F}_q^n \mid \forall \mathbf{c} \in \mathcal{C} : \mathbf{c}' \cdot \mathbf{c} = 0\}$ der* duale Code *von $\mathcal{C}$.*

Klarerweise ist $\mathcal{C}^\perp$ immer ein linearer Code. $(\mathcal{C}^\perp)^\perp$ ist die lineare Hülle von $\mathcal{C}$.Ist insbesondere $\mathcal{C}$ linear, so gilt: $(\mathcal{C}^\perp)^\perp = \mathcal{C}$ und $\dim(\mathcal{C}) = n - \dim(\mathcal{C}^\perp)$.

Ist $\mathcal{C}$ ein linearer Code, so nennt man eine Erzeugermatrix von $\mathcal{C}^\perp$ eine *Checkmatrix* von $\mathcal{C}$. Es gilt somit $\mathbf{c} \in \mathcal{C}$ genau dann, wenn für alle Zeilen $\mathbf{b}$ der Checkmatrix gilt: $\mathbf{c} \cdot \mathbf{b} = 0$. Dies liefert eine effektive Methode zu „checken“, ob ein Wort ein Codewort ist oder nicht. Im Gegensatz dazu muß man im nichtlinearen Fall im allgemeinen ein Wort mit allen Codeworten vergleichen. Hat $\mathcal{C}$ Minimaldistanz d, so heißt das, daß d die kleinste Zahl ist, so daß es d Spalten der Checkmatrix gibt, die linear abhängig sind. Und umgekehrt: sind je beliebige $d-1$ Spalten der Checkmatrix linear unabhängig, so ist $\mathcal{C}$ ein Code der Distanz d. Wir haben also gesehen:

Bemerkung 1.6 *$\mathcal{C}$ ist ein linearer, q-ärer $[n,k,d]$ genau dann, wenn $\mathcal{C}^\perp$ ein lineares $OA(d-1,n,q)$ der Dimension $n-k$ ist.*

Definition 1.7 *Sei $\mathcal{C} \subset V^n$ ein Code, Die Zahlen*

$$A_i(\mathcal{C}) = A_i := \frac{1}{|\mathcal{C}|}|\{(\mathbf{a},\mathbf{b}) \in \mathcal{C}^2 | \mathrm{d}(\mathbf{a},\mathbf{b}) = i\}|$$

heißen die Distanzzahlen *von $\mathcal{C}$. Das Tupel $(A_0, A_1, \ldots, A_n)$ heißt die* Distanzverteilung *von $\mathcal{C}$. Das* Distanzpolynom *ist definiert als*

$$W_{\mathcal{C}}(X,Y) := \sum_{i=0}^{n} A_i X^{n-i} Y^i$$

Für lineare (und additive) Codes ist A_i gerade die Anzahl der Worte vom Gewicht i, also insbesondere eine natürliche Zahl. Im allgemeinen sind die Distanzzahlen nichtnegative rationale Zahlen. Aus der Distanzverteilung läßt sich die Minimaldistanz ablesen. Die Minimaldistanz d ist die kleinste positive Zahl, für die A_d größer als Null ist. Außerdem überlegt man sich leicht, daß $A_0 = 1$ und $\sum_{i=0}^{n} A_i = |\mathcal{C}|$ gilt.

Satz 1.8 (MacWilliams [23]) *Sei $\mathcal{C}$ ein linearer, q-ärer Code mit Distanzpolynom $W_{\mathcal{C}}(X,Y)$. Dann ist das Distanzpolynom des dualen Codes*

$$W_{\mathcal{C}^\perp}(X,Y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(X + (q-1)Y, X - Y)$$

Auch für beliebige v-äre Codes kann man die *MacWilliams-Transformierte* (A'_i) der Distanzverteilung definieren durch: $\frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(X+(v-1)Y, X-Y) = \sum_{i=0}^{n} A'_i X^{n-i} Y^i$. Delsarte [13] hat die MacWilliams-Transformation für beliebige v-äre Codes untersucht. Ein Hauptergebnis Delsartes ist, daß auch die A'_i nichtnegative rationale Zahlen sind. Diese Tatsache kann man benutzen, um mittels linearer Programmierung gute obere Schranken für Codes zu berechnen. Delsarte [14] folgend definieren wir die vier fundamentalen Parameter eines Codes.

Definition 1.9 *Sei (A_i) die Distanzverteilung eines v-ären Codes. Sei (A'_i) die daraus mittels MacWilliams-Transformation erhaltene Verteilung. Wir nennen (A'_i) die* duale Distanzverteilung*. Wir definieren außerdem folgende Parameter:*

$\mathrm{d}(\mathcal{C})$ *die kleinste Zahl* > 0 *für die* $A_d \neq 0$

$\mathrm{d}'(\mathcal{C})$ *die kleinste Zahl* > 0 *für die* $A'_{d'} \neq 0$

$s(\mathcal{C})$ *die Anzahl der* $i > 0$ *mit* $A_i \neq 0$

$s'(\mathcal{C})$ *die Anzahl der* $i > 0$ *mit* $A'_i \neq 0$

$\mathrm{d}(\mathcal{C})$ *heißt die* Minimaldistanz, $\mathrm{d}'(\mathcal{C})$ *die* duale Distanz, $s(\mathcal{C})$ *die* Anzahl der Distanzen *und* $s'(\mathcal{C})$ *die* äußere Distanz *des Codes* $\mathcal{C}$.

Im linearen Fall haben wir durch Bemerkung 1.6 gesehen, daß $d'(\mathcal{C})-1$ gerade die maximale Stärke des Codes ist. Man beachte, daß im nichtlinearen Fall die duale Distanzverteilung im allgemeinen nicht die Distanzverteilung des dualen Codes ist. Im Fall, daß v keine Primzahlpotenz ist, ist der duale Code nicht einmal definiert. Um so überraschender ist ein weiteres Ergebnis Delsartes [14]:

Satz 1.10 *Ist* $\mathcal{C}$ *ein Code der dualen Distanz* d'*, so ist* $d'-1$ *die Stärke von* $\mathcal{C}$.

Die dualen Distanzzahlen lassen sich mittels einer Familie orthogonaler Polynome, der Kravtchoukpolynome, einfach ausdrücken.

Definition 1.11 *Für natürliche Zahlen* n *und* v *definieren wir das* Kravtchoukpolynom *vom Grad* $k \leq n$ *durch*

$$K_k(X;n,v) = K_k(X) := \sum_{j=0}^{k}(-1)^j \binom{X}{j}\binom{n-X}{k-j}(v-1)^{k-j}$$

Die Kravtchoukpolynome erfüllen folgende Relation

$$\sum_{k=0}^{n} K_k(i)X^{n-k}Y^k = (X+(v-1)Y)^{n-i}(X-Y)^i \quad , \quad 1 \leq i \leq n$$

und damit sehen wir leicht, daß $A'_k = \frac{1}{|\mathcal{C}|}\sum_{i=0}^{n} A_i K_k(i)$.

1.2 Einige einfache Eigenschaften und Konstruktionen

Bemerkung 1.12 *Sei* $\mathcal{C}$ *ein* v*-ärer* $[n,|\mathcal{C}|,d]$ *der Stärke* t *über dem Alphabet* V.

i) $\mathcal{C}$ *ist auch ein* v*-ärer* $[n,|\mathcal{C}|,\bar{d}]$ *für* $\bar{d} \leq d$ *und hat Stärke* $\bar{t}$ *für* $\bar{t} \leq t$.

ii) Streicht man beliebige l *Worte in* $\mathcal{C}$*, so erhält man einen* v*-ären* $[n,|\mathcal{C}|-l,d]$. *Hängt man beliebige* l *Koordinaten an* $\mathcal{C}$ *an, so erhält man einen* v*-ären* $[n+l,|\mathcal{C}|,d]$.

iii) Streicht man aus $\mathcal{C}$ *beliebige* $l \leq d$ *Koordinaten, so erhält man einen* v*-ären* $[n-l,|\mathcal{C}|,d-l]$ *der Stärke* t.

iv) Streicht man aus $\mathcal{C}$ eine Koordinate und betrachtet alle Wort aus $\mathcal{C}$, die dort einen festen Eintrag $x \in V$ haben, so bilden diese Worte, ohne die gestrichene Koordinate, einen v-ären $[n-1, K, d]$. Dieser hat Stärke $t-1$. Für mindestens eine Wahl von x ist $K \geq \lceil |\mathcal{C}|/v \rceil$. Dies tritt im linearen Fall für alle x mit Gleichheit ein. Der durch $x = 0$ entstehende Code ist wieder linear und wir erhalten somit einen $[n-1, k-1, d]$, wobei $k = \dim(\mathcal{C})$.

Wenden wir Punkt iii) $d-1$ mal auf einen v-ären $[n, |\mathcal{C}|, d]$ an, so erhält man einen v-ären $[n-d+1, |\mathcal{C}|, 1]$. Dessen Worte sind alle verschieden, also gilt $|\mathcal{C}| \leq v^{n-d+1}$. Man nennt dies die *Singleton Schranke*. Im Fall, daß $\mathcal{C}$ ein linearer $[n, k, d]$ ist, vereinfacht sich die Ungleichung zu $k \leq n - d + 1$. Codes, die die Singleton Schranke erreichen, nennt man *MDS Codes* (maximum distance separable).

Sei $\mathcal{C}$ ein linearer, binärer $[n, k, d]$ dessen Distanz d ungerade ist. Verlängert man die Codeworte von $\mathcal{C}$ um eine Koordinate und wählt deren Eintrag, so daß das Gewicht des jeweiligen Wortes gerade wird, so erhält man einen linearen, binären $[n+1, k, d+1]$. Man nennt diese Operation einen *parety check* anfügen. Die inverse Operation wird durch Punkt iii) garantiert.

Satz 1.13 (Groneick Grosse [20]) *Sei $\mathcal{C}$ ein linearer, q-ärer $[n, k, d]$, $\mathbf{a} \in \mathcal{C}$ ein Wort vom Gewicht $w < dq/(q-1)$, so gibt es einen linearen, q-ären Code*

$$[n - w, k - 1, d - \lfloor w(q-1)/q \rfloor].$$

Beweis: ObdA sei $\mathbf{a} = (1, \ldots, 1, 0, \ldots, 0)$. Wähle $\mathbf{a}$ als erste Zeile einer Erzeugermatrix von $\mathcal{C}$. Sei $\overline{\mathcal{C}}$ der Code der von der Matrix erzeugt wird die man erhält, wenn man in der Erzeugermatrix von $\mathcal{C}$ die erste Zeile und die ersten w Spalten streicht.
$\overline{\mathcal{C}}$ hat Dimension k-1, denn sonst gäbe es in $\mathcal{C}$ ein Wort $\mathbf{b} \neq \mathbf{0}$ das höchstens an den ersten w Stellen nichtverschwindende Einträge hat und das nicht von der Form $\lambda\mathbf{a}$, $\lambda \in \mathbb{F}_q^\times$ ist. Mindestens ein Eintrag $\lambda \neq 0$ kommt in $\mathbf{b}$ mindestens $d/(q-1)$ mal vor. Damit hätte $\mathbf{b} - \lambda\mathbf{a} \in \mathcal{C}$ Gewicht höchstens $w - d/(q-1)$. Nach Voraussetzung ist aber $w < dq/(q-1)$ und damit $w - d/(q-1) < d$, Widerspruch.
Sei $\overline{\mathbf{b}}$ ein Wort vom Gewicht $i < d$ in $\overline{\mathcal{C}}$. Das Urbild $\mathbf{b}$ in $\mathcal{C}$ hat in den ersten w Koordinaten mindestens einen Eintrag $\lambda \in \mathbb{F}_q^\times$, der $(d-i)/(q-1)$ mal vorkommt. Damit gilt für das Gewicht von $\mathbf{b} - \lambda\mathbf{a} \in \mathcal{C}$:

$$w - (d-i)/(q-1) + i \geq \mathrm{wt}(\mathbf{b} - \lambda\mathbf{a}) \geq d$$

und damit für i, daß $i \geq d - w(q-1)/q$. Somit ist $d_{\overline{\mathcal{C}}} \geq d - w(q-1)/q$. ■

Setzt man im obigen Satz $w = d_{\mathcal{C}}$ die Minimaldistanz des Codes, so erhält man den Satz von Griesmer [19].

Folgerung 1.14 (Griesmer) *Ist $\mathcal{C}$ ein linearer, q-ärer $[n,k,d]$, so gibt es einen linearen, q-ären $[n-d,k-1,\lceil d/q\rceil]$.*

Beweis: Nach Satz 1.13 bekommen wir einen $[n-d_{\mathcal{C}},k-1,d_{\mathcal{C}}-\lfloor d_{\mathcal{C}}(q-1)/q\rfloor]=[n-d_{\mathcal{C}},k-1,\lceil d_{\mathcal{C}}/q\rceil]$. Da $d\le d_{\mathcal{C}}$ ist dieser nach Bemerkung 1.12 auch ein $[n-d,k-1,\lceil d/q\rceil]$ ■

Durch Iteration des Griesmerschritts erhält man eine untere Schranke für die Länge eines linearen Codes.

Folgerung 1.15 (Griesmer Schranke) *Ist $\mathcal{C}$ ein linearer, q-ärer $[n,k,d]$, so gilt:*

$$n\ge\sum_{i=0}^{k-1}\lceil d/q^i\rceil$$

Im Rest des Abschnitts wollen wir uns Konstruktionen anschauen, die mehrere Codes zu einem neuen zusammensetzen. Die Konstruktionen X4, X [24] und XX [1] sind, obwohl sie allgemein gelten, hier nur für lineare Codes formuliert, da dann die Formulierung klarer ist. Man beachte, daß die Beweise nur benutzen, daß das Alphabet ein Vektorraum ist, so daß sich die Beweise der Konstruktionen unverändert für die Codes in Abschnitt 4 verwenden lassen.

Bemerkung 1.16 (Konstruktion X4) *Seien $\mathcal{C}'\subset\mathcal{C}$ lineare, q-äre Codes mit den Parametern $[n,k-\kappa,d']$ bzw. $[n,k,d]$. Seien $\overline{\mathcal{C}'}\subset\overline{\mathcal{C}}$ lineare, q-äre $[\bar n,\bar k-\kappa,\bar d']$ bzw. $[\bar n,\bar k,\bar d]$. Dann existiert ein linearer, q-ärer $[n+\bar n,k+\bar k-\kappa,\mathrm{Min}(d',\bar d',d+\bar d)]$.*

Beweis: Die $(n+\bar n,k+\bar k-\kappa)$-Matrix M sei wie folgt definiert. Betrachte die Einschränkung M_1 von M auf die ersten n Spalten. Die ersten $k-\kappa$ Zeilen von M_1 seien eine Erzeugermatrix von $\mathcal{C}'$, die ersten k Zeilen von M_1 seien eine Erzeugermatrix von $\mathcal{C}$ und die letzten $\bar k-\kappa$ Zeilen von M_1 seien Null. Sei M_2 die Einschränkung von M auf die letzten $\bar n$ Spalten. Die letzten $\bar k-\kappa$ Zeilen von M_2 seien eine Erzeugermatrix von $\overline{\mathcal{C}'}$, die letzten $\bar k$ Zeilen von M_2 seien eine Erzeugermatrix von $\overline{\mathcal{C}}$ und die ersten $k-\kappa$ Zeilen von M_2 seien Null. Sei $\mathbf{c}$ ein Codewort ungleich Null des von M erzeugten Codes. Ist $\mathbf{c}$ im Erzeugnis der ersten $k-\kappa$ Zeilen, so ist $\mathrm{wt}(\mathbf{c})\ge d'$. Ist $\mathbf{c}$ im Erzeugnis der letzten $\bar k-\kappa$ Zeilen, so ist $\mathrm{wt}(\mathbf{c})\ge\bar d'$. Ansonsten ist $\mathrm{wt}(\mathbf{c})\ge d+\bar d$ ■

Bemerkung 1.17 (Konstruktion X) *Seien $\mathcal{C}'\subset\mathcal{C}$ lineare, q-äre Codes mit den Parametern $[n,k',d']$ bzw. $[n,k,d]$. Existiert außerdem ein linearer, q-ärer Hilfscode $\overline{\mathcal{C}}$ mit den Parametern $[\bar n,k-k',\bar d]$, so existiert ein linearer, q-ärer $[n+\bar n,k,\mathrm{Min}(d',d+\bar d)]$.*

Konstruktion X erhält man aus Konstruktion X4 indem man $\overline{\mathcal{C}'} = \mathbf{0}$ setzt, also die letzten $\bar{k} - \kappa$ Zeilen der Matrix M nicht auftreten. Eine weitere nützliche Konstruktion erhält man durch zweifache Anwendung von Konstruktion X. Es handelt sich um eine leichte Verallgemeinerung von Alltops Konstruktion XX [1].

Bemerkung 1.18 (Konstruktion XX) *Seien $\mathcal{C}_1, \mathcal{C}_2 \subset \mathcal{C}$ lineare, q-äre Codes mit den Parametern $[n, k-\kappa_1, d+\delta_1]$, $[n, k-\kappa_2, d+\delta_2]$ bzw. $[n, k, d]$. Sei $\mathcal{C}' = \mathcal{C}_1 \cap \mathcal{C}_2$ ein $[n, k-\kappa', d+\delta']$. Seien $\overline{\mathcal{C}}_1$ $\overline{\mathcal{C}}_2$ lineare, q-äre $[\bar{n}_1, \kappa_1, \bar{d}_1]$ bzw. $[\bar{n}_2, \kappa_2, \bar{d}_2]$. Dann existiert auch ein linearer, q-ärer $[n+\bar{n}_1+\bar{n}_2, k, d+\mathrm{Min}(\bar{d}_1+\bar{d}_2, \delta_1+\bar{d}_2, \delta_2+\bar{d}_1, \delta')]$.*

Beweis: Man wende Konstruktion X auf das Paar $\mathcal{C}_1 \subset \mathcal{C}$ mit Hilfscode $\overline{\mathcal{C}}_1$ an und erhält $\mathcal{D}$, einen $[n+\bar{n}_1, k, \mathrm{Min}(d+\bar{d}_1, d+\delta_1)]$. Das Bild $\mathcal{D}_2$ von $\mathcal{C}_2$ in diesem Code ist ein $[n+\bar{n}_1, k-\kappa_2, \mathrm{Min}(d+\delta_2+\bar{d}_1, d+\delta')]$. Wendet man auf das Paar $\mathcal{D}_2 \subset \mathcal{D}$ mit Hilfscode $\overline{\mathcal{C}}_2$ wiederum Konstruktion X an, so erhält man die Behauptung ■

Bemerkung 1.19 (Konkatenation) *Existiert ein v-ärer $[n, K, d]$ und ein u-ärer $[n', K' = v, d']$, so auch ein u-ärer $[nn', K, dd']$.*

Beweis: Sei ϕ eine Bijektion vom Alphabet des v-ären $[n, K, d]$ auf die Codeworte des u-ären $[n', K' = v, d']$. Dann ist das ϕ-Bild des v-ären $[n, K, d]$ ein u-ärer $[nn', K, \delta]$. Im Urbild unterscheiden sich zwei Worte an mindestens d Stellen, jede dieser Stellen wurde im Bild durch zwei verschiedene Worte des u-ären $[n', K' = v, d']$ ersetzt, also ist die Distanz zweier verschiedener Worte im Bild mindestens dd' ■

Sind die Ausgangscodes linear mit $v = q^r$ und $u = q$, so kann man es auch so einrichten, daß der konkatenierte Code linear ist (siehe Bemerkung 4.2).

Bemerkung 1.20 (Konstruktion Y1) *Sei $\mathcal{C}$ ein linearer, q-ärer $[n, k, d]$, $\mathbf{c}' \in \mathcal{C}^\perp$ mit $\mathrm{wt}(\mathbf{c}') = d'$. Dann gibt es einen linearen, q-ären $[n-d', k-d'+1, d]$*

Beweis: Sei M eine Checkmatrix von $\mathcal{C}$ mit erster Zeile $\mathbf{c}'$. Betrachten wir die Matrix M', die wir aus M erhalten indem wir den Träger von $\mathbf{c}'$ streichen. Somit ist die erste Zeile von M' Null. Streichen wir also die erste Zeile von M', so sind immer noch je $d-1$ Spalten linear unabhängig. Die Matrix M' ohne die erste Zeile ist somit eine Checkmatrix eines $[n-d', k-d'+1, d]$. ■

1.3 Ein erstes Ergebnis

Nun noch eine untere Schranke für lineare Codes. Sei $V(n, i)$ die Anzahl der Vektoren in F_q^n vom Gewicht höchstens i. Klarerweise ist

$$V(n, i) = \sum_{j=0}^{i} \binom{n}{j} (q-1)^j.$$

Ist $\mathcal{C}$ ein linearer, q-ärer $[n, k-1, d]$, so liefert $q^{k-1}V(n, d-1)$ eine obere Schranke für die Zahl der Worte in $\mathbb{F}_{q^n}$, die Distanz $< d$ zu einem Codewort haben. Ist $q^{k-1}V(n, d-1) < q^n$, so gibt es also einen Vektor $\mathbf{v} \in \mathbb{F}_{q^n}$, der von jedem Element von $\mathcal{C}$ Distanz $\geq d$ hat. Also gilt $\mathrm{wt}(\mathbf{v} - \mathbf{c}) \geq d$ für alle $\mathbf{c} \in \mathcal{C}$. Damit hat der von $\mathcal{C}$ und $\mathbf{v}$ erzeugte Code Distanz $\geq d$. Wendet man diese Überlegung rekursiv an, beginnend mit dem trivialen $[n, 1, d]$, so liefert dies die Gilbert-Varshamov-Schranke:

Satz 1.21 (Gilbert-Varshamov-Schranke) *Ist $V(n, d-1) < q^{n-k+1}$, so gibt es einen linearen, q-ären $[n, k, d]$.*

Betrachtet man den zugehörigen dualen Code, so erhält man ein Schranke, die immer besser ist als die Gilbert-Varshamov-Schranke. Man findet diese Schranke z.B. als Übungsaufgabe bei MacWilliams/Sloane ([24], Seite 34).

Satz 1.22 *Ist $V(n-1, d-2) < q^{n-k}$, so gibt es einen linearen, q-ären $[n, k, d]$.*

Beweis: Die Anzahl der Vektoren in $\mathbb{F}_q^{n-k}$, die als Linearkombination von höchstens $t-1$ Vektoren aus einer Menge von $n-1$ Vektoren geschrieben werden kann, ist höchstens $\sum_{j=0}^{t-1} \binom{n-1}{j}(q-1)^j$, also höchstens $V(n-1, t-1)$. Sei $\mathcal{A}$ die Checkmatrix eines q-ären linearen $[n-1, k-1, d]$. Insbesondere sind je $d-1$ Spalten von $\mathcal{A}$ linear unabhängig. Ist $V(n-1, d-2) < q^{n-k}$, so gibt es nach obiger Überlegung einen Vektor $\mathbf{v} \in \mathbb{F}_q^{n-k}$, der von jeder $(d-2)$-Menge von Spaltenvektoren von $\mathcal{A}$ linear unabhängig ist. Also ist die Matrix, die man aus $\mathcal{A}$ durch Anhängen der Spalte $\mathbf{v}$ erhält, eine Erzeugermatrix eines OA der Stärke $d-1$, d.h. die Checkmatrix eines $[n, k, d]$. Da $V(n, \cdot)$ offensichtlich monoton mit n steigt, kann man sich durch rekursive Anwendung des obigen Arguments von der Forderung der Existenz eines $[n-1, k-1, d]$ befreien und erhält die Behauptung.

Daß Satz 1.22 immer besser ist als Satz 1.21, ist äquivalent mit $qV(n-1, d-2) < V(n, d-1)$. Nach Definition ist $V(n-1, d-2)$ die Zahl der Vektoren der Länge $n-1$ und Gewicht $\geq d-2$. Verlängert man diese Vektoren um eine Koordinate und ergänzt sie dort auf alle q möglichen Weisen, so erhält man $qV(n-1, d-2)$ verschiedene Vektoren der Länge n und Gewicht $\leq d-1$. Da wir $n \geq d$ haben, sind dies offensichtlich nicht alle solche Vektoren ■

Sei $\mathcal{C}$ ein linearer, q-ärer $[n-i, k-i, d+\delta]$. Ist $V(n-1, d-2) < q^{n-k}$, so kann man nach obiger Überlegung $\mathcal{C}$ in einen $[n, k, d]$ einbetten. Wendet man auf diesen Code Bemerkung 1.17 (Konstruktion X) an, so erhält man:

Satz 1.23 *Sei $V(n-1, d-2) < q^{n-k}$ und gibt es einen linearen, q-ären Code $\mathcal{C} = [n-i, k-i, d+\delta]$ und einen linearen, q-ären Code $\mathcal{D} = [e, i, \delta]$, so gibt es einen linearen, q-ären Code $\mathcal{E} = [n+e, k, d+\delta]$.*

Dies läßt sich noch etwas verbessern. Sei $\mathcal{C}$ ein linearer, q-ärer $[n,k,d]$ mit Checkmatrix $\mathcal{A}$. Die Zahl der Vektoren, die sich als Linearkombination von höchstens s Spalten von $\mathcal{A}$ schreiben lassen, sei $N_{\mathcal{C}}(s)$. Im ersten Schritt der Konstruktion benutzen wir die Abschätzung $N_{\mathcal{C}}(s) \leq \mathrm{Min}(V(n,s), q^{n-k})$. Sei nun $\mathcal{A}'$ die 2×2 Blockmatrix mit Einträgen oben links $\mathcal{A}$, unten rechts die $i \times i$ Einheitsmatrix und Nullmatrizen auf der Nebendiagonale. Das so definierte $\mathcal{A}'$ ist die Checkmatrix von $\mathcal{C}'$, des mit i Nullen verlängerten Codes $\mathcal{C}$, also eines $[n+i,k,d]$. Wir erhalten eine Abschätzung für $N_{\mathcal{C}'}(t)$:

$$N_{\mathcal{C}'}(t) \leq N(i,t,\mathcal{C}) := \sum_{s=0}^{t} \binom{i}{s} (q-1)^s N_{\mathcal{C}}(t-s)$$

Das Wachstum von $N(i,t,\mathcal{C})$ läßt sich wie folgt abschätzen.

$$\begin{aligned}
N(i+1,t,\mathcal{C}) &= \sum_{s=0}^{t} \binom{i+1}{s} (q-1)^s N_{\mathcal{C}}(t-s) \\
&= N_{\mathcal{C}}(t) + \sum_{s=1}^{t} \binom{i}{s} (q-1)^s N_{\mathcal{C}}(t-s) + \sum_{s=1}^{t} \binom{i}{s-1} (q-1)^s N_{\mathcal{C}}(t-s) \\
&= N(i,t,\mathcal{C}) + (q-1) \sum_{s=0}^{t-1} \binom{i}{s} (q-1)^s N_{\mathcal{C}}(t-(s+1)) \\
&\leq N(i,t,\mathcal{C}) + (q-1) \sum_{s=0}^{t-1} \binom{i}{s} (q-1)^s N_{\mathcal{C}}(t-s) \\
&= qN(i,t,\mathcal{C}) - \binom{i}{t} (q-1)^t
\end{aligned}$$

Die vorletzte Zeile folgt aus der Tatsache, daß die $N_{\mathcal{C}}(s)$ monoton steigen. Damit haben wir gesehen:

$$N(i+1,t,\mathcal{C}) = \begin{cases} < qN(i,t,\mathcal{C}) & \text{falls } i \geq t \\ \leq qN(i,t,\mathcal{C}) & \text{falls } i < t \end{cases} \tag{1}$$

Sei $d' \leq d$. Gibt es ein i, für das $N(i,d'-2,\mathcal{C}) < q^{n+i-k}$ ist, so erhält man mit dem selben Argument wie in Satz 1.22 die Existenz von $\mathcal{C}''$, einem $[n+i+1, k+1, d']$, der $\mathcal{C}$ als Teilcode enthält. Wegen (1) tritt dieser Fall ein, wenn man i nur groß genug wählt. Wendet man die Konstruktion nun auf $\mathcal{C}''$ an, so kann man $N_{\mathcal{C}''}(s)$ mit $N_{\mathcal{C}''}(s) \leq \mathrm{Min}(N(i+1,s,\mathcal{C}), q^{n+i-k})$ abschätzen. Damit bekommen wir folgenden Satz:

Satz 1.24 *Existiere $\mathcal{C}_1$, ein linearer, q-ärer $[n,k,d]$. Sei $d' \leq d$. Definiere $N(i,t,\mathcal{C}_1) := \mathrm{Min}(V(n,t), q^{n-k})$, $\iota(1) := 0$ und seien, für $j \geq 1$:*

$$N(i,t,\mathcal{C}_{j+1}) := \sum_{s=0}^{t} \binom{i}{s} (q-1)^s \,\mathrm{Min}(N(\iota(j)+1, t-s, \mathcal{C}_j), q^{n-k+\sum_{e=1}^{j}\iota(e)})$$

$$\iota(j+1) := \mathrm{Min}\{i \in I\!N \mid N(i,d'-2,\mathcal{C}_{j+1}) < q^{n+i-k+\sum_{e=1}^{j}\iota(e)}\}.$$

Dann existiert C_{j+1}, ein $[n+\sum_{l=2}^{j+1}\iota(l)+j, k+j, d']$, der C_j enthält. Existiert außerdem ein linearer, q-ärer Code $\mathcal{D}=[e,j,\delta]$ mit $\delta \le d-d'$, so erhält man mit Konstruktion X einen linearen, q-ären Code $E=[n+\sum_{l=2}^{j+1}\iota(l)+j+e, k+j, d'+\delta]$.

Ein Beispiel: Nach [8] gibt es $\mathcal{C}_1$, einen quaternären [39,24,9]. Es ist:

$$146824822 = V(39,5) < 1073741824 = 4^{15} < 2525276989 = V(39,6)$$

Also ist $N(i,t,\mathcal{C}_1) = V(39,t)$ für $t \le 5$ und $=4^{15}$ für $t > 5$.

$$\begin{aligned} N(2,7,\mathcal{C}_2) &= \sum_{s=0}^{7}\binom{2}{s}3^s N(1,7-s,\mathcal{C}_1) \\ &= (1+2\cdot 3)\cdot 4^{15} + 3^2 \cdot V(39,5) \\ &= 8837616166 < 17179869184 = 4^{17} \end{aligned}$$

Damit ist $\iota(2) = 2$ und es gibt also $\mathcal{C}_2$, einen $[42,25,9]$. Es ist $N(3,7,\mathcal{C}_2) = 14888416951 < 4^{17}$, damit ist $N(0,7,\mathcal{C}_3) = N(3,7,\mathcal{C}_2) < 4^{17}$. Also ist $\iota(3) = 0$ und damit gibt es $\mathcal{C}_3$, einen $[43,26,9]$. Dieser ist nach [8] neu.

Man erhält durch Sätze 1.23 und 1.24, bei systematischer Suche durch die in den folgenden Abschnitten beschriebenen Codes und durch Andries Brouwers' Datenbank linearer binärer, ternärer und quaternärer Codes [8], viele Verbesserungen in derselben. Eine Auflistung der so entstandenen neuen Codes, deren Parameter im Bereich der Datenbank liegen, ist im Anhang A zu finden.

Obwohl man die in den obigen Sätzen postulierten Codes im Prinzip auch konstruieren kann, sollte man sie im allgemeinen als reine Existenzaussage betrachten. Das Problem liegt nicht darin, einen passenden Vektor zum Verlängern zu finden, eine Zufallssuche würde in den meisten Fällen nach wenigen Schritten zum Erfolg führen, sondern zu entscheiden, ob der Vektor zum Verlängern geeignet ist. Dazu muß man im allgemeinen die Vereinigung der Erzeugnisse aller t-Teilmengen von Spalten des Ausgangscodes berechnen, was wegen des schnellen Wachstums von $\binom{n}{t}$ für große t nicht mehr praktikabel ist. Außerdem benötigt man eine Erzeugermatrix des Ausgangscodes. Falls der Code aus der Datenbank stammt, so ist diese auch nicht immer zu rekonstruieren.

Für einige Codes kleiner Distanz, die in den folgenden Abschnitten behandelt werden, hat der Autor systematisch mit dem Computer nach Verlängerungen der Checkmatrix gesucht, die neue Codes liefern und die besser sind als durch die obigen Sätze garantiert. Diese werden in Abschnitt 6 behandelt.

1.4 Zyklische Codes

Ein Code $\mathcal{C}$ der Länge n heißt *zyklisch*, wenn es eine zyklische Permutation π der Ordnung n gibt, so daß für $\mathbf{c} = (c_i) \in \mathcal{C}$ stets auch $(c_{\pi(i)}) \in \mathcal{C}$ ist. Durch

Umbenennung der Koordinaten kann man ObdA annehmen, daß $\pi = (0, \ldots, n-1)$ ist. Für zyklische, lineare, q-äre Codes ist es üblich, ein Codewort $\mathbf{c} = (c_i) \in \mathcal{C}$ mit dem Polynom $c(X) := \sum_{i=0}^{n-1} c_i X^i \in \mathbb{F}_q[X]/(X^n-1)$ zu identifizieren. In dieser Schreibweise ist $\mathcal{C}$ zyklisch genau dann, wenn für alle $c(X) \in \mathcal{C}$ auch $Xc(X) \in \mathcal{C}$ ist. Wir erhalten folgende Charakterisierung der linearen zyklischen Codes.

Satz 1.25 *$\mathcal{C}$ ist genau dann ein zyklischer linearer Code, wenn $\mathcal{C}$ ein Ideal in $\mathbb{F}_q[X]/(X^n-1)$ ist.*

Beweis: Ist $\mathcal{C}$ ein Ideal in $\mathbb{F}_q[X]/(X^n-1)$, so gilt insbesondere: Für alle $c(X) \in \mathcal{C}$ ist auch $Xc(X) \in \mathcal{C}$, also ist $\mathcal{C}$ zyklisch. Die Linearität folgt unmittelbar daraus, daß $\mathcal{C}$ ein Ideal ist.
Umgekehrt: Da $\mathcal{C}$ zyklisch ist, ist für alle $c(X) \in \mathcal{C}$ auch $Xc(X) \in \mathcal{C}$ und damit $X^i c(X) \in \mathcal{C}$. Da $\mathcal{C}$ linear ist, ist damit $f(X)c(X) \in \mathcal{C}$ für alle $f \in \mathbb{F}_q[X]/(X^n-1)$. Damit (und wegen der Linearität) ist $\mathcal{C}$ ein Ideal in $\mathbb{F}_q[X]/(X^n-1)$ ■

$\mathcal{C}$ wird vom normierten Polynom kleinsten Grades $g(X) \in \mathcal{C}$ erzeugt; g heißt das *Generatorpolynom* von $\mathcal{C}$. Das Generatorpolynom g ist ein Teiler von $X^n - 1$. Jedes Codewort von $\mathcal{C}$ läßt sich somit eindeutig in der Form $f\ g$ schreiben, mit $\operatorname{grad}(f)\operatorname{grad}(g) \leq n-1$. Damit bekommen wir als Dimension von $\mathcal{C}$:

$$\dim_{\mathbb{F}_q} \mathcal{C} = n - \operatorname{grad}(g). \tag{2}$$

Sei $f_1(X) \cdots f_t(X)$ die Zerlegung von $X^n - 1$ in irreduzible Faktoren. Sei im folgenden immer $\operatorname{ggt}(n, q) = 1$. Damit sind die f_i alle verschieden und somit kann man das Generatorpolynom als ein beliebiges Produkt verschiedener f_i wählen.

Sei ζ eine n-te Einheitswurzel in einem geeigneten Erweiterungskörper $\mathbb{F}_{q^r}$. ζ heißt *Nullstelle des zyklischen Codes* $\mathcal{C}$, wenn $c(\zeta) = 0$ für alle $\mathbf{c} \in \mathcal{C}$. Sei f der irreduzible Faktor von $X^n - 1$, welcher ζ als Nullstelle hat. Es sei also f das Minimalpolynom von ζ in $\mathbb{F}_q[X]$. Dann ist ζ Nullstelle von $\mathcal{C}$ genau dann, wenn f das Generatorpolynom von $\mathcal{C}$ teilt. Also ist ein zyklischer linearer Code durch Vorgabe seiner Nullstellen eindeutig bestimmt. Das Generatorpolynom ist das kgV der Minimalpolynome der Nullstellen.

Bemerkung 1.26 *Sei $\mathcal{C}$ der lineare zyklische Code mit Generatorpolynom g und sei $h = (X^n-1)/g$. Dann ist h das Generatorpolynom des Codes, den man erhält, wenn man die Codeworte von $\mathcal{C}^\perp$ von hinten nach vorne liest.*

Beweis: Sei $f = \sum_{i=0}^{n-1} f_i X^i \in \mathcal{C}$ und $f' = \sum_{i=0}^{n-1} f'_i X^i \in \mathcal{C}'$, dem von h erzeugten Code. Also ist $f(X) = p(X)g(X)$ und $f'(X) = p'(X)h(X)$. Da $h(X)g(X) = X^n - 1$ ist, ist der Koeffizient von X^{n-1} von ff', also $\sum_{i=0}^{n-1} f_i f'_{n-1-i} = \sum_{i=0}^{n-1} p_i p'_{n-1-i} = 0$, denn der Grad von $p(X)p'(X)$ ist höchstens $2(n-1) - n = n - 2$. Damit ist der rückwärts gelesene $\mathcal{C}'$ in $\mathcal{C}^\perp$ enthalten. Da $h(X)g(X) = X^n - 1$ ist, haben $\mathcal{C}$ und $\mathcal{C}'$ nach (2) komplementäre Dimension; somit muß der rückwärts gelesene $\mathcal{C}'$ gleich $\mathcal{C}^\perp$ sein ■

Definition 1.27 *Sei ζ eine primitive n-te Einheitswurzel. Der lineare zyklische Code $\mathcal{C}$ mit den Nullstellen $\zeta^i, wo \quad l \leq i \leq l+d-2$ heißt* BCH-Code *der designten Distanz d. Ist $l = 1$, so heißt $\mathcal{C}$* narrow-sense *BCH-Code. Ist $n = q^m - 1$, also ζ ein primitives Element von $\mathbb{F}_{q^m}$, so heißt $\mathcal{C}$ ein* primitiver *BCH-Code. Ist $n = q - 1$, so heißt $\mathcal{C}$* Reed-Solomon-Code*. Die Abkürzung BCH steht für die Anfangsbuchstaben der Namen der Erfinder Bose, Chaudhuri und Hocquenghem.*

Ein BCH-Code der designten Distanz d hat mindestens d als Minimaldistanz. Dies wird sich auch als Folgerung von Satz 2.13 ergeben.

2 Eine Verallgemeinerung der BCH-Codes

2.1 $\mathbb{F}_q$-Linearität

Im folgenden wird es sich als nützlich herausstellen, eine Sorte von Codes bzw. Orthogonaler Arrays zur Verfügung zu haben, die etwas weniger Struktur als die linearen Codes haben, denen aber noch viele der nützlichen Eigenschaften der linearen Codes erhalten bleiben.

Definition 2.1 *Sei $\mathcal{C}$ ein q^r-ärer Code / OA der Länge n, dessen Alphabet $\mathbf{V}$ ein $\mathbb{F}_q$-Vektorraum ist, also $\dim_{F_q}(\mathbf{V}) = r$.*

$\mathcal{C}$ heiße $\mathbb{F}_q$-linear falls *$\mathcal{C}$ ein $\mathbb{F}_q$-Untervektorraum von $\mathbf{V}^n$ ist, wenn also die Summe zweier Codeworte wieder ein Codewort ist, sowie für $\lambda \in \mathbb{F}_q$, das λ-fache eines Codewortes wieder ein Codewort ist.*

Die Dimension k von $\mathcal{C}$ sei definiert als die Dimension von $\mathcal{C}$ als $\mathbb{F}_q$-Vektorraum. Ist d die Distanz von $\mathcal{C}$, so schreiben wir $\mathcal{C} = [n, k, d]$.

Auf den Codeworten von $\mathcal{C}$ sei ein Skalarprodukt $\langle \cdot, \cdot \rangle : \mathbf{V}^n \times \mathbf{V}^n \longrightarrow \mathbb{F}_q$, durch

$$\langle \mathbf{c}, \mathbf{d} \rangle := \sum_{i=1}^{n} (c_i, d_i) \tag{3}$$

definiert, mit $\mathbf{c} = (c_i), \mathbf{d} = (d_i) \in \mathbf{V}^n$, wobei $(\cdot, \cdot)$ ein nichtausgeartetes Skalarprodukt auf $\mathbf{V}$ ist.

$\mathcal{C}^{\perp\!\!\!\perp} := \{\mathbf{d} \in \mathbf{V}^n | \langle \mathbf{d}, \mathbf{c} \rangle = 0$ für alle $\mathbf{c} \in \mathcal{C}\}$ ist das orthogonale Komplement bezüglich dieses Skalarproduktes. $\mathcal{C}^{\perp\!\!\!\perp}$ ist damit ebenfalls $\mathbb{F}_q$-linear. Wir nennen $\mathcal{C}^{\perp\!\!\!\perp}$ ebenfalls den dualen Code *von $\mathcal{C}$.*

Man überlegt sich leicht:

Bemerkung 2.2 *Ein $\mathbb{F}_q$-linearer, q-ärer Code $\mathcal{C}$ ist ein linearer, q-ärer Code. In diesem Fall ist $\langle \cdot, \cdot \rangle$ das Standardskalarprodukt auf $\mathbb{F}_q^n$ und $\mathcal{C}^{\perp\!\!\!\perp}$ damit dasselbe wie $\mathcal{C}^{\perp}$.*

Ein linearer, q^r-ärer Code ist ein $\mathbb{F}_q$-linearer, q^r-ärer Code.

Die Minimaldistanz eines $\mathbb{F}_q$-linearen Codes ist das Minimalgewicht eines Codewortes ungleich Null.

Wie im linearen bekommen wir:

Satz 2.3 *Sei $\mathcal{C}$ ein $\mathbb{F}_q$-lineares $OA(t, n, q^r)$ der Dimension $nr - k$, so ist*

i) $\mathcal{C}^{\perp\!\!\!\perp}$ ein $\mathbb{F}_q$-linearer, q^r-ärer Code mit den Parametern $[n, k, t + 1]$.

ii) $(\mathcal{C}^{\perp\!\!\!\perp})^{\perp\!\!\!\perp} = \mathcal{C}$.

Beweis: i) Annahme: es gäbe ein Codewort $\mathbf{c} = (c_i) \in \mathcal{C}^{\perp\!\!\!\perp}\backslash\{0\}$ mit $\mathrm{wt}(\mathbf{c}) \leq t$. Sei ObdA $c_i = 0$ für $i > t$ und $c_1 \in \mathbf{V}\backslash\{0\}$. Da $\mathcal{C}$ ein OA der Stärke t ist, gibt es ein $\mathbf{a} = (a_i) \in \mathcal{C}$ mit $a_1 \in \mathbf{V}\backslash\{0\}$ beliebig und $a_i = 0$ für $2 \leq i \leq t$. Damit ist $\langle \mathbf{a}, \mathbf{c}\rangle := \sum_{i=1}^{n}(a_i, c_i) = (a_1, c_1)$. Da $(\cdot,\cdot)$ nicht ausgeartet ist, gibt es ein $a_1 \in \mathbf{V}$, so daß $\langle \mathbf{a}, \mathbf{c}\rangle \neq 0$. Dies ist aber ein Widerspruch zur Annahme $\mathbf{c} \in \mathcal{C}^{\perp\!\!\!\perp}$. Also sind Minimalgewicht und Minimaldistanz in $\mathcal{C}^{\perp\!\!\!\perp}$ mindestens $t + 1$.

ii) Fassen wir $\mathbf{V}^n$ als $\mathbb{F}_q^{rn}$ auf, so ist $\langle\cdot,\cdot\rangle$ ein nichtausgeartetes Skalarprodukt auf $\mathbb{F}_q^{rn}$ und damit gilt für jeden Untervektorraum $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$ $(\mathcal{C}^{\perp\!\!\!\perp})^{\perp\!\!\!\perp} = \mathcal{C}$ ■

Nach Satz 1.10 ist die duale Distanz eines Codes gerade eins, plus die Stärke des Codes. Damit haben wir in Analogie zum linearen Fall das folgende Ergebnis: Ist $\mathcal{C}$ ein $\mathbb{F}_q$-linearer, q^r-ärer $[n, k, d]$ mit dualer Distanz d', so ist $\mathcal{C}^{\perp\!\!\!\perp}$ ein $\mathbb{F}_q$-linearer, q^r-ärer $[n, nr - k, d']$ mit dualer Distanz d. Es gilt sogar wie im linearen Fall:

Satz 2.4 *Ist $\mathcal{C}$ ein $\mathbb{F}_q$-linearer Code mit dualer Distanzverteilung (A'_i), so ist (A'_i) die Distanzverteilung des dualen $\mathbb{F}_q$-linearen Codes $\mathcal{C}^{\perp\!\!\!\perp}$.*

Beweis: Man kann den Beweis aus dem linearen Fall mit leichten Modifikationen übernehmen. Wir werden uns hier an dem Beweis von van Lint [22] orientieren. Erinnern wir uns: das Alphabet $\mathbf{V}$ ist ein $\mathbb{F}_q$-Vektorraum und sei $\langle \mathbf{u}, \mathbf{v}\rangle$ das durch (3) definierte Skalarprodukt. Sei χ ein nichttrivialer Charakter von $(\mathbb{F}_q, +)$. Definiere $g(\mathbf{u}) := \sum_{\mathbf{v}\in\mathbf{V}^n} \chi(\langle \mathbf{u}, \mathbf{v}\rangle) X^{n-\mathrm{wt}(\mathbf{v})} Y^{\mathrm{wt}(\mathbf{v})}$. Dann gilt:

$$\sum_{\mathbf{u}\in\mathcal{C}} g(\mathbf{u}) = \sum_{\mathbf{u}\in\mathcal{C}} \sum_{\mathbf{v}\in\mathbf{V}^n} \chi(\langle \mathbf{u}, \mathbf{v}\rangle) X^{n-\mathrm{wt}(\mathbf{v})} Y^{\mathrm{wt}(\mathbf{v})} = \sum_{\mathbf{v}\in\mathbf{V}^n} X^{n-\mathrm{wt}(\mathbf{v})} Y^{\mathrm{wt}(\mathbf{v})} \sum_{\mathbf{u}\in\mathcal{C}} \chi(\langle \mathbf{u}, \mathbf{v}\rangle)$$

Ist $\mathbf{v} \in \mathcal{C}^{\perp\!\!\!\perp}$, so ist $\chi(\langle \mathbf{u}, \mathbf{v}\rangle) = 1$ und damit die innere Summe gleich $|\mathcal{C}|$. Ist $\mathbf{v} \notin \mathcal{C}^{\perp\!\!\!\perp}$ fest gewählt, so nimmt, wegen der $\mathbb{F}_q$-Linearität von $\mathcal{C}$, in der inneren Summe $\langle \mathbf{u}, \mathbf{v}\rangle$ jeden Wert in $\mathbb{F}_q$ gleich oft an und damit ist die innere Summe gleich Null. Wir haben also gezeigt

$$\sum_{\mathbf{u}\in\mathcal{C}} g(\mathbf{u}) = |\mathcal{C}| \sum_{\mathbf{v}\in\mathcal{C}^{\perp}} X^{n-\mathrm{wt}(\mathbf{v})} Y^{\mathrm{wt}(\mathbf{v})} = |\mathcal{C}| \sum_{i=0}^{n} A'_i X^{n-i} Y^i = |\mathcal{C}| W_{\mathcal{C}^{\perp}}(X, Y) \tag{4}$$

Setze die Gewichtsfunktion auf $\mathbf{V}$ fort, durch $\mathrm{wt}(0) = 0$ und $\mathrm{wt}(v) = 1$ für $v \in \mathbf{V}\backslash\{0\}$. Damit haben wir für $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbf{V}^n$, daß $\mathrm{wt}(\mathbf{v}) = \sum_{i=1}^{n} \mathrm{wt}(v_i)$

und erhalten

$$\begin{aligned} g(\mathbf{u}) &= \sum_{\mathbf{v}\in\mathbf{V}^n} \chi(\langle \mathbf{u},\mathbf{v}\rangle) X^{n-\mathrm{wt}(\mathbf{v})} Y^{\mathrm{wt}(\mathbf{v})} \\ &= \sum_{(v_1,\dots,v_n)\in\mathbf{V}^n} \chi(\sum_{i=1}^{n}(u_i,v_i)) X^{n-\sum_{i=1}^n \mathrm{wt}(v_i)} Y^{\sum_{i=1}^n \mathrm{wt}(v_i)} \\ &= \sum_{(v_1,\dots,v_n)\in\mathbf{V}^n} \prod_{i=1}^{n} \chi((u_i,v_i)) X^{1-\mathrm{wt}(v_i)} Y^{\mathrm{wt}(v_i)} \\ &= \prod_{i=1}^{n} \sum_{v\in\mathbf{V}} \chi((u_i,v)) X^{1-\mathrm{wt}(v)} Y^{\mathrm{wt}(v)} \end{aligned}$$

Ist in dem letzten Ausdruck $u_i = 0$, so ist die innere Summe gleich $X+(|\mathbf{V}|-1)Y$. Ist $u_i \neq 0$, so ist die innere Summe gleich $X + \sum_{v\in\mathbf{V}\setminus\{0\}} \chi((u_i,v))Y$. Da $(\cdot,\cdot)$ ein nichtausgeartetes Skalarprodukt auf $\mathbf{V}$ ist, nimmt (u_i,v) jeden Wert in $\mathbb{F}_q$ gleich oft an, wenn v ganz $\mathbf{V}$ durchläuft. Damit ist $\sum_{v\in\mathbf{V}} \chi((u_i,v)) = 0$ und da $\chi(0) = 1$ haben wir $\sum_{v\in\mathbf{V}\setminus\{0\}} \chi((u_i,v)) = -1$. Somit ist

$$g(\mathbf{u}) = (X + (|\mathbf{V}|-1)Y)^{n-\mathrm{wt}(\mathbf{u})}(X-Y)^{\mathrm{wt}(\mathbf{u})}.$$

Damit erhalten wir unter Benutzung der durch Gleichung (4) gelieferten Identität wie behauptet

$$\sum_{\mathbf{u}\in\mathcal{C}} (X + (|\mathbf{V}|-1)Y)^{n-\mathrm{wt}(\mathbf{u})}(X-Y)^{\mathrm{wt}(\mathbf{u})} = W_{\mathcal{C}}(X + (|\mathbf{V}|-1)Y, X-Y) = |\mathcal{C}| W_{\mathcal{C}^\perp}(X,Y)$$

■

Nun betrachten wir Teilcodes, die wir als Einschränkung von $\mathbb{F}_q$-linearen Codes auf Untervektorräume des Alphabets erhalten, sowie Bilder unter $\mathbb{F}_q$-linearen Abbildungen von $\mathbb{F}_q$-linearen OAs. Dies war auch die Motivation zur Definition der $\mathbb{F}_q$-linearen Codes/OA. Denn startet man hier mit linearen Codes/OA, so bekommt man im allgemeinen nur $\mathbb{F}_q$-lineare Codes/OA als Ergebnisse.

Sei das Alphabet $\mathbf{V}$ ein r-dimensionaler $\mathbb{F}_q$-Vektorraum. Sei $\mathcal{C}$ ein $\mathbb{F}_q$-linearer, q^r-ärer $[n,k,d]$. Klarerweise ist jeder Untervektorraum von $\mathcal{C}$ wieder ein $\mathbb{F}_q$-linearer Code der Distanz (mindestens) d. Interessant sind besonders solche Teilräume die zu einem Code über einem kleineren Alphabet führen. Sei $\mathbf{U} \subset \mathbf{V}$ ein Untervektorraum der Dimension s. Betrachten wir nun den Untervektorraum $\mathcal{C}|_{\mathbf{U}} := \mathcal{C} \cap \mathbf{U}^n$, so ist $\mathcal{C}|_{\mathbf{U}}$ ein $\mathbb{F}_q$-linearer, q^s-ärer $[n,k',d]$, mit $k' \leq k$.

Sei andererseits ϕ eine $\mathbb{F}_q$-lineare Abbildung von $\mathbf{V}$ mit $\dim_{\mathbb{F}_q} \mathrm{Bild}(\phi) = s$. Setze ϕ auf $\mathbf{V}^n$ komponentenweise fort, so ist $\phi(\mathcal{C})$, das Bild unter ϕ eines $\mathbb{F}_q$-linearen $OA(t,n,q^r)$, ein $\mathbb{F}_q$-linearer $OA(t,n,q^s)$. (Denn wegen der Linearität haben die Urbilder von $\phi(x)$ für alle x gleich viele Elemente). ϕ ist ein $\mathbb{F}_q$-Vektorraum-Homomorphismus. Damit gilt für die Dimensionen $\dim_{\mathbb{F}_q} \mathcal{C} = \dim_{\mathbb{F}_q} \phi(\mathcal{C}) + \dim_{\mathbb{F}_q} \mathrm{Kern}_\phi(\mathcal{C})$. Hier ist $\mathrm{Kern}_\phi(\mathcal{C})$, unter Benutzung obiger Notation, gerade $\mathcal{C}|_{\mathrm{Kern}(\phi)}$. Damit haben wir folgenden Satz:

Satz 2.5 *Sei* $\mathbf{V}$ *ein* $\mathbb{F}_q$*-Vektorraum und* $\mathcal{C}$ *ein* $\mathbb{F}_q$*-lineares,* q^r*-äres* $OA(d'-1,n,q^r)$ *der Dimension* k *über dem Alphabet* $\mathbf{V}$*. Sei* ϕ *eine* $\mathbb{F}_q$*-lineare Abbildung von* $\mathbf{V}$ *mit* $\dim_{F_q}\mathrm{Bild}(\phi) = s$ *und sei* $\dim_{F_q}(\mathcal{C}|_{\mathrm{Kern}\,\phi}) =: \rho$*. Dann ist also* $\mathcal{C}|_{\mathrm{Kern}\,\phi}$ *ein* $\mathbb{F}_q$*-linearer,* q^{r-s}*-ärer* $[n,\rho,d]$ *und* $\phi(\mathcal{C})$ *ein* $\mathbb{F}_q$*-linearer,* q^s*-ärer* $OA(d'-1,n,q^s)$ *der Dimension* $k-\rho$*.*

Man erhält auch eine Verallgemeinerung von Delsartes Theorem welches im Falle linearer Codes besagt, daß $\mathrm{tr}(\mathcal{C}^\perp) = (\mathcal{C}|_{F_q})^\perp$.

Bemerkung 2.6 *Zu jedem Teilraum* $K \subset \mathbb{F}_{q^r}$ *gibt es eine surjektive* $\mathbb{F}_q$*-lineare Abbildung* $\phi : V = \mathbb{F}_{q^r} \to K$ *und ein nichtausgeartetes Skalarprodukt* $(\cdot,\cdot)$ *auf* K*, so daß für jeden* q^r*-ären, linearen Code* $\mathcal{C}$ *gilt:*

$$\phi(\mathcal{C}^\perp) = (\mathcal{C}|_K)^{\perp\!\!\!\perp}$$

Hier ist $^{\perp\!\!\!\perp}$ *das durch* $\langle\cdot,\cdot\rangle$ *definierte orthogonale Komplement in* K^n *und* $(\cdot,\cdot)$ *das innere Skalarprodukt, welches gemäß der Definition von* $\langle\cdot,\cdot\rangle$ *(Gleichung (3)) verwendet wird.*

Beweis: Sei K ein $\mathbb{F}_q$-linearer Unterraum von $\mathbb{F}_{q^r}$ mit Basis $\alpha_1,\ldots,\alpha_s \in \mathbb{F}_{q^r}$. Definiere ϕ durch $\phi(x) := \sum_{i=1}^s \alpha_i \,\mathrm{tr}(\alpha_i x)$, wobei $\mathrm{tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ die Spur ist. Damit ist ϕ eine $\mathbb{F}_q$-lineare Abbildung mit $\mathrm{Bild}(\phi) = K$.

Sei $(\cdot,\cdot)$ ein nichtausgeartetes $\mathbb{F}_q$-Skalarprodukt auf K, für das $\alpha_1,\ldots,\alpha_s$ eine Orthonormalbasis wird. Dieses Skalarprodukt benutzen wir jetzt als inneres Skalarprodukt bei der Definition des Skalarproduktes $\langle\cdot,\cdot\rangle$ auf K^n (Gleichung (3)). Das ($\mathbb{F}_{q^r}$-lineare) Standardskalarprodukt in $(\mathbb{F}_{q^r})^n$ bezeichnen wir mit „$\cdot$“ und $\mathcal{C}^\perp$ sei das orthogonale Komplement bezüglich dieses Skalarproduktes.

1) Es gilt: $\phi(\mathcal{C}^\perp) \subseteq (\mathcal{C}|_K)^{\perp\!\!\!\perp}$. Also ist zu zeigen, daß $\forall \mathbf{c} \in \mathcal{C}^\perp \forall \mathbf{d} \in \mathcal{C}|_K$: $\langle\phi(\mathbf{c}),\mathbf{d}\rangle = 0$. Da $\mathbf{d} = (d_j) \in \mathcal{C}|_K$ ist, gibt es $\lambda_{i,j} \in \mathbb{F}_q$, so daß $d_j = \sum_{i=1}^s \alpha_i\lambda_{i,j}$ ist. Damit ist:

$$\begin{aligned}
\langle\phi(\mathbf{c}),\mathbf{d}\rangle &= \sum_{j=1}^n (\sum_{i=1}^s \alpha_i \,\mathrm{tr}(\alpha_i c_j), \sum_{k=1}^s \alpha_k\lambda_{k,j}) \\
&= \sum_{j=1}^n \sum_{i=1}^s \mathrm{tr}(\alpha_i c_j)\lambda_{i,j} \quad (\text{ wegen der Orthonormalität}) \\
&= \sum_{j=1}^n \sum_{i=1}^s \mathrm{tr}(\alpha_i c_j \lambda_{i,j}) = \sum_{j=1}^n \mathrm{tr}(c_j \sum_{i=1}^s \alpha_i\lambda_{i,j}) \\
&= \sum_{j=1}^n \mathrm{tr}(c_j d_j) = \mathrm{tr}(\sum_{j=1}^n c_j d_j) = \mathrm{tr}(\mathbf{c}\cdot\mathbf{d}) = \mathrm{tr}(0) = 0
\end{aligned}$$

2) Es ist $\phi(\mathcal{C}^\perp) \supseteq (\mathcal{C}|_K)^{\perp\!\!\!\perp} \Leftrightarrow \phi(\mathcal{C}^\perp)^{\perp\!\!\!\perp} \subseteq (\mathcal{C}|_K)$. Angenommen dem wäre nicht so. Dann gibt es ein $\mathbf{u} \in \phi(\mathcal{C}^\perp)^{\perp\!\!\!\perp} \backslash \mathcal{C}|_K$. Da $\phi(\mathcal{C}^\perp)^{\perp\!\!\!\perp} \subseteq K^n \subseteq \mathbb{F}_{q^r}^n$ ist, ist dies äquivalent mit $\mathbf{u} \in \phi(\mathcal{C}^\perp)^{\perp\!\!\!\perp} \backslash \mathcal{C}$. Da $(\mathcal{C}^\perp)^\perp = \mathcal{C}$ gibt es ein $\mathbf{v} \in \mathcal{C}^\perp$ mit $\mathbf{u} \cdot \mathbf{v} \neq 0$ und somit ist für alle $\gamma \in \mathbb{F}_{q^r}^\times$ auch $\gamma\mathbf{v} \in \mathcal{C}^\perp$ mit $\mathbf{u} \cdot \gamma\mathbf{v} \neq 0$. Da $\mathbf{u} \in K^n$ ist, können wir $\mathbf{u} = (u_i)$ schreiben, wo $u_i = \sum_{j=1}^s \alpha_j \mu_{j,i}$ mit $\mu_{j,i}$ in $\mathbb{F}_q$. Damit haben wir :

$$\begin{aligned}
\langle \mathbf{u}, \phi(\gamma\mathbf{v}) \rangle &= \sum_{i=1}^n (u_i, \phi(\gamma v_i)) \\
&= \sum_{i=1}^n (\sum_{j=1}^s \alpha_j \mu_{j,i}, \sum_{k=1}^s \alpha_k \operatorname{tr}(\alpha_k \gamma v_i)) \\
&= \sum_{i=1}^n \sum_{j=1}^s \mu_{j,i} \operatorname{tr}(\alpha_j \gamma v_i) = \operatorname{tr}(\sum_{i=1}^n \sum_{j=1}^s \mu_{j,i} \alpha_j \gamma v_i) \\
&= \operatorname{tr}(\sum_{i=1}^n u_i \gamma v_i) = \operatorname{tr}(\gamma \mathbf{u} \cdot \mathbf{v})
\end{aligned}$$

Da die Spur nicht die Nullabbildung ist und $\mathbf{u} \cdot \mathbf{v} \neq 0$, gibt es ein γ für das $\operatorname{tr}(\gamma \mathbf{u} \cdot \mathbf{v}) \neq 0$. Andererseits ist $\langle \mathbf{u}, \phi(\gamma\mathbf{v}) \rangle = 0$ weil $\mathbf{u} \in \phi(\mathcal{C}^\perp)^{\perp\!\!\!\perp}$ und $\gamma\mathbf{v} \in \mathcal{C}^\perp$ist. Dies ist ein Widerspruch, also gilt $\phi(\mathcal{C}^\perp) \supseteq (\mathcal{C}|_K)^{\perp\!\!\!\perp}$.
Punkt 1) und 2) zusammen liefern die Behauptung ■

2.2 Die verallgemeinerten BCH-Codes

In diesem Abschnitt wollen wir für eine bestimmte Klasse von Ausgangscodes die durch Satz 2.5 gelieferten Codes genauer untersuchen.

Definition 2.7 *Sei $w|(q^r-1)$, sei $\mathbf{W} \subset \mathbb{F}_{q^r}$ die Gruppe der w-ten Einheitswurzeln in $\mathbb{F}_{q^r}$ und $\zeta \in \mathbf{W}$ eine primitive w-te Einheitswurzel. Setze für $t < w$*
$\mathcal{P}(w,l,t) := \{f \in \mathbb{F}_{q^r}[X]/(X^w-1) \,|\, f \equiv X^l \cdot h \in \mathbb{F}_{q^r}[X],\ grad(h) < t\}$
$\mathcal{A}(w,l,t) := \{\mathbf{a} = (a_1, \ldots, a_w) \in \mathbb{F}_{q^r}^w \,|\, a_i = f(\zeta^i), f \in \mathcal{P}(w,l,t), 1 \leq i \leq w\}$

Verschiedene Vertreter einer Nebenklasse aus $\mathbb{F}_{q^r}[X]/(X^w-1)$ haben für alle Elemente in $\mathbf{W}$ dieselben Funktionswerte, da $\zeta^w - 1 = 0$ für alle $\zeta \in \mathbf{W}$. Also lassen sich Aussagen über die Funktionswerte von Elementen aus $\mathcal{P}(w,l,t)$ an Stellen aus $\mathbf{W}$, durch Prüfen der Aussage an einem beliebigen Vertretersystem, z.B. $X^l \cdot h \in \mathbb{F}_{q^r}[X]$, $grad(h) < t$, verifizieren. Somit erhalten wir eine etwas modifizierte Lagrange-Interpolation für $\mathcal{P}(w,l,t)$.

Bemerkung 2.8 *Ein Polynom in $\mathcal{P}(w,l,t)$ ist durch seine Funktionswerte an t verschiedenen Stellen in $\mathbf{W}$ eindeutig bestimmt.*

Beweis: Eindeutigkeit: Seien f, g zwei Polynome der Form $X^l \cdot h \in I\!F_{q^r}[X]$, $grad(h) < t$, die an t verschiedenen Stellen in $\mathbf{W}$ dieselben Werte annehmen, so hat das Polynom $f - g$ mindestens t verschiedene Nullstellen ungleich 0 und eine l-fache Nullstelle an 0, also mit Vielfachheiten gezählt mindestens $t+l$ Nullstellen. Da $\text{grad}(f-g) < t+l$ ist $f - g$ das Nullpolynom und damit $f = g$.

Existenz: Zu einem t-Tupel $(x_1, \ldots, x_t)$ verschiedener Elemente aus $\mathbf{W}$ definiere $L_i(X) := \left(\frac{X}{x_i}\right)^l \prod_{\substack{j=1,\ldots,t \\ j\neq i}} \frac{X-x_j}{x_i-x_j}$. Sei y_i der vorgeschriebene Funktionswert an x_i, so ist $f = \sum_{i=1}^{t} y_i \cdot L_i(X)$ ein Polynom mit $f(x_i) = y_i$ der Form $X^l \cdot h \in I\!F_{q^r}[X]$, $grad(h) < t$ ■

Damit können wir leicht die Parameter von $\mathcal{A}(w, l, t)$ als Code oder OA bestimmen.

Lemma 2.9 *$\mathcal{A}(w, l, t)$ ist ein zyklischer linearer, q^r-ärer $[w, t, w-t+1]$ und ein lineares $OA(t, w, q^r)$ der Dimension t. Desweiteren ist der duale Code $\mathcal{A}(w, l, t)^\perp = \mathcal{A}(w, w-l+1, w-t)$.*

Beweis: Die Linearität folgt unmittelbar aus der Definition von $\mathcal{A}(w, l, t)$. Die Stärke und Minimaldistanz folgen unmittelbar aus der Bemerkung 2.8. Sei ζ eine primitive w-te Einheitswurzel. Ist $\mathbf{a} = (a_i) = (f(\zeta^i)) \in \mathcal{A}(w, l, t)$, so ist $\mathbf{b} = (b_i) = (f(\zeta^{i+1}))$ eine zyklische Permutation des Codewortes $\mathbf{a}$. Das Wort $\mathbf{b}$ wird durch das Polynom $g(X) := f(\zeta X) \in \mathcal{P}(w, l, t)$ erzeugt, liegt also auch in $\mathcal{A}(w, l, t)$.

Sei $\mathbf{a} = (a_i) = (f(\zeta^i)) \in \mathcal{A}(w, l, t)$ und $\mathbf{b} = (b_i) = (g(\zeta^i)) \in \mathcal{A}(w, w-l+1, w-t)$. Dann ist

$$\begin{aligned}
\mathbf{a} \cdot \mathbf{b} &= \sum_{i=1}^{w} f(\zeta^i) g(\zeta^i) \\
&= \sum_{i=1}^{w} (\zeta^{il} \sum_{j=0}^{t-1} f_j \zeta^{ij})(\zeta^{i(w-l+1)} \sum_{k=0}^{w-t-1} g_k \zeta^{ik}) \\
&= \sum_{j=0}^{t-1} f_j \sum_{k=0}^{w-t-1} g_k \sum_{i=1}^{w} \zeta^{(j+k+1)i}
\end{aligned}$$

Wegen der Grade von f und g gilt $1 \leq j + k + 1 < w$, also ist $\zeta^{j+k+1} \neq 1$ und eine w-te Einheitswurzel. Damit ist $\sum_{i=1}^{w} (\zeta^{j+k+1})^i = 0$, also auch $\mathbf{a} \cdot \mathbf{b} = 0$ für alle $\mathbf{a} \in \mathcal{A}(w, l, t)$ und $\mathbf{b} \in \mathcal{A}(w, w-l+1, w-t)$. Da $\mathcal{A}(w, l, t)$ und $\mathcal{A}(w, w-l+1, w-t)$ komplementäre Dimensionen haben ist $\mathcal{A}(w, l, t)^\perp = \mathcal{A}(w, w-l+1, w-t)$. ■

Die Codes $\mathcal{A}(w, l, t)$ sind spezielle BCH-Codes. Diese haben die Eigenschaft MDS ($n + 1 = k + d$). Für $w = q^r - 1$ erhält man Reed-Solomon-Codes. Bei diesen ist diese Art der Darstellung üblich. Einen Beweis dafür, daß es sich um BCH-Codes handelt, wird sich als Spezialfall von Satz 2.13 ergeben.

Definition 2.10 *Sei ϕ eine $\mathbb{F}_q$-lineare Abbildung von $\mathbb{F}_{q^r} \cong \mathbb{F}_q^r$ auf einen Untervektorraum. Definiere* $\rho(\phi, w, l, t) := \dim_{F_q} \mathcal{A}(w, l, t)|_{\operatorname{Kern}\phi}$

Aus den Sätzen 2.3 und 2.5 erhalten wir

Lemma 2.11 *Sei ϕ eine $\mathbb{F}_q$-lineare Abbildung von $\mathbb{F}_{q^r} \cong \mathbb{F}_q^r$ auf einen Untervektorraum der Dimension s. Sei $\mathcal{A} = \mathcal{A}(w, l, t)$. Dann gilt das folgende:*

$\mathcal{A}|_{\operatorname{Kern}\phi}$ ist ein $\mathbb{F}_q$-linearer, q^{r-s}-ärer $[w, \rho(\phi, w, l, t), w - t + 1]$,
$\phi(\mathcal{A})$ ein $\mathbb{F}_q$-lineares $OA(t, w, q^s)$ der Dimension $rt - \rho(\phi, w, l, t)$,

$(\mathcal{A}|_{\operatorname{Kern}\phi})^{\perp\!\!\!\perp}$ ein $\mathbb{F}_q$-lineares $OA(w-t, w, q^{r-s})$ der Dimension $(r-s)w-\rho(\phi, w, l, t)$,
$\phi(\mathcal{A})^{\perp\!\!\!\perp}$ ein $\mathbb{F}_q$-linearer, q^s-ärer $[w, sw - rt + \rho(\phi, w, l, t), t + 1]$.

Der Bestimmung von $\rho(\phi, w, l, t)$ ist der nächste Abschnitt gewidmet. Hier noch einige nützliche Eigenschaften:

Satz 2.12 *Seien ϕ, ψ $\mathbb{F}_q$-lineare Abbildungen von $\mathbb{F}_{q^r} \cong \mathbb{F}_q^r$.*

i) Ist $\alpha \in \mathbb{F}_{q^r}^\times$ und $\operatorname{Kern}(\psi) = \alpha \operatorname{Kern}(\phi)$*, so gilt:*

$$\rho(\phi, w, l, t) = \rho(\psi, w, l, t)$$

ii) Zu jedem ϕ gibt es ein ψ mit $\operatorname{Bild}(\psi) = \operatorname{Kern}(\phi)$*, so daß gilt:*

$$\dim_{F_q}(\operatorname{Bild}(\phi))w + \rho(\phi, w, l, t) = rt + \rho(\psi, w, w - l + 1, w - t)$$

Beweis: i) Sei $\alpha \in \mathbb{F}_{q^r}^\times$. Für die $\mathbb{F}_q$-linearen Abbildungen ϕ_α, $\phi_\alpha(x) := \phi(\alpha^{-1}x)$, gilt $\operatorname{Kern}(\phi_\alpha) = \alpha \operatorname{Kern}(\phi)$. Da $\mathcal{C} := \mathcal{A}(w, l, t)$ ein linearer, q^r-ärer Code ist, ist mit $\mathbf{c} \in \mathcal{C}$ auch $\alpha\mathbf{c} \in \mathcal{C}$ für alle $\alpha \in \mathbb{F}_{q^r}$. Also haben $\mathcal{C}|_{\operatorname{Kern}(\phi)}$ und $\mathcal{C}|_{\alpha \operatorname{Kern}(\phi)}$ die gleiche Dimension, d.h. $\rho(\phi, w, l, t) = \rho(\phi_\alpha, w, l, t)$. Nach Definition erhält man für alle ϕ mit demselben Kern, denselben Wert für $\rho(\phi, w, l, t)$. Damit folgt die Behauptung.

ii) Sei $K = \operatorname{Kern}(\phi)$ mit $\dim_{F_q}(K) = r - s$. Sei ψ mit $\operatorname{Bild}(\psi) = K$ und das Skalarprodukt auf K^n gemäß Bemerkung 2.6 gewählt, so daß $\psi(\mathcal{C}^\perp) = (\mathcal{C}|_K)^{\perp\!\!\!\perp}$ gilt. Hier haben wir $\mathcal{C} = \mathcal{A}(w, l, t)$ also $\mathcal{C}^\perp = \mathcal{A}(w, w - l + 1, w - t)$ nach Lemma 2.9. Nach Definition ist $\rho(\phi, w, l, t) = \dim(\mathcal{A}(w, l, t)|_K)$, also bekommen wir mit Lemma 2.11 $(r - s)w - \rho(\phi, w, l, t) = \dim((\mathcal{A}(w, l, t)|_K)^{\perp\!\!\!\perp}) = \dim(\psi(\mathcal{A}(w, w - l + 1, w - t)) = r(w - t) - \rho(\psi, w, w - l + 1, w - t)$. Damit haben wir $sw + \rho(\phi, w, l, t) = rt+\rho(\psi, w, w-l+1, w-t)$ für dieses spezielle Skalarprodukt. Da aber ρ als Dimension eines Vektorraums unabhängig von der Wahl des Skalarproduktes immer denselben Wert annimmt, folgt die Behauptung. ■

Satz 2.13 *Sei ϕ eine $\mathbb{F}_q$-lineare Abbildung von $\mathbb{F}_{q^r}$ nach$\mathbb{F}_q$, $\zeta \in \mathbb{F}_{q^r}$ eine primitive w-te Einheitswurzel. Dann ist $\phi(\mathcal{A}(w,l,t))^{\perp\!\!\!\perp} = \phi(\mathcal{A}(w,l,t))^{\perp}$ der BCH-Code mit den Nullstellen $\zeta^i, \quad l \le i \le l+t-1$.*

Beweis: Sei $\zeta \in \mathbb{F}_{q^r}$ eine primitive w-te Einheitswurzel. Jedes Codewort $\mathbf{c}$ von $\phi(\mathcal{A}(w,l,t))$ läßt sich als $\mathbf{c} = \mathbf{c}_f = (\phi(f(\zeta^i))\,|1 \le i \le w)$ schreiben, mit geeignetem $f = X^l \sum_{j=0}^{t-1} a_j X^j \in \mathcal{P}(w,l,t)$. Jede $\mathbb{F}_q$-lineare Abbildung $\phi : \mathbb{F}_{q^r} \to \mathbb{F}_q$ läßt sich in der Form $\phi(x) = \mathrm{tr}(\alpha x)$ mit $\alpha \in \mathbb{F}_{q^r}^{\times}$ schreiben, wobei $\mathrm{tr}(x) = \sum_{i=0}^{r-1} x^{q^i}$ die Spur von $\mathbb{F}_{q^r} \to \mathbb{F}_q$ ist. Da mit c_f auch $c_{\alpha f}$ ein Codewort ist, können wir ObdA $\phi = \mathrm{tr}$ setzen. Da das Bild der Spur $\mathbb{F}_q$ ist, ist nach Bemerkung 2.2 $\mathrm{tr}(\mathcal{A}(w,l,t))$ linear und $\mathrm{tr}(\mathcal{A}(w,l,t))^{\perp\!\!\!\perp} = \mathrm{tr}(\mathcal{A}(w,l,t))^{\perp}$. Nach Lemma 2.9 ist $\mathcal{A}(w,l,t)$ zyklisch. Dasselbe gilt auch für $\mathrm{tr}(\mathcal{A}(w,l,t))$. Wir erhalten eine Darstellung von $\mathbf{c}$ als Polynom $\mathbf{c}(y)$, analog wie im Abschnitt 1.4 für zyklische Codes definiert, durch $\mathbf{c}(y) := \sum_{i=1}^{w} c_i y^{w-i} = \sum_{i=1}^{w} \mathrm{tr}(f(\zeta^i)) y^{w-i}$. Dies ist als *Mattson-Solomon-Polynom* bekannt. Es handelt sich um einen Isomorphismus zwischen den Ringen $(\mathbb{F}_q[X]/(X^w-1), +, *)$ und $(\mathbb{F}_q[X]/(X^w-1), +, \circ)$, wobei $*$ die Polynommultiplikation modulo X^w-1 ist und $\circ$ die Multiplikation der Koeffizienten der Monome komponentenweise. Damit bekommen wir:

$$\begin{aligned} c(\zeta^k) &= \sum_{i=1}^{w} \sum_{m=0}^{r-1} \sum_{j=0}^{t-1} (a_j \zeta^{i(l+j)})^{q^m} \zeta^{-ik} \\ &= \sum_{m=0}^{r-1} \sum_{j=0}^{t-1} a_j^{q^m} \sum_{i=1}^{w} \zeta^{i((l+j)q^m-k)} \\ &= \sum_{m=0}^{r-1} \sum_{j=0}^{t-1} a_j^{q^m} w \delta_{(l+j)q^m,k} \end{aligned}$$

Hier ist das Kroneckersymbol $\delta_{x,y} = 1$, falls $x \equiv y \mod w$ und Null sonst. Sei $Z(j) := \{jq^l \mod w \,|\, l \in \mathbb{Z}/(r)\}$. Die Beziehung $(l+j)q^m \equiv k \mod w$ kann nur gelten wenn $(l+j) \in Z(k)$ ist. Wähle das Vertretersystem für $Z(k)$ in $[l, l+w-1]$. Ist also das minimale Element von $Z(k)$ größer als $l+t-1$, so ist $c(\zeta^k) = 0$. Ist $l+t-1$ kleinergleich dem minimalen Element in $Z(k)$, so gibt es immer ein $\mathbf{c} \in \mathrm{tr}(\mathcal{A}(w,l,t))$, so daß $\mathbf{c}(\zeta^k) \neq 0$ ist, sonst hätte man eine lineare Abhängigkeit der Körperautomrphismen.

$\mathrm{tr}(\mathcal{A}(w,l,t))$, rückwärts gelesen, ist also der zyklische Code mit den Nullstellen ζ^i mit $i \notin \bigcup_{j=l}^{l+t-1} Z(j)$. Damit ist $\mathrm{tr}(\mathcal{A}(w,l,t))^{\perp}$ der zyklische Code mit den Nullstellen ζ^i mit $i \in \bigcup_{j=l}^{l+t-1} Z(j)$ (Bemerkung 1.26). Da es reicht, aus jeder zyklotomischen Nebenklasse mindestens eine Nullstelle zu nehmen, ist der Code auch schon durch die Nullstellen $\zeta^i, \quad l \le i \le l+t-1$ eindeutig bestimmt. Nach Definition 1.27 ist $\mathrm{tr}(\mathcal{A}(w,l,t))^{\perp}$ also der BCH-Code mit den Nullstellen ζ^i, wo $l \le i \le l+t-1$. ■

Für spätere Anwendungen ist es wichtig zu wissen, wie die $\mathcal{A}$'s ineinander enthalten sind. Nach Definition ist $\mathcal{A}(w,l,t) \subset \mathcal{A}(w,l',t')$, falls die Restklassen von

$l, \ldots, l+t-1$ modulo w in den Restklassen von $l', \ldots, l'+t'-1$ modulo w enthalten sind. Beachten wir, daß nach Definition $0 \leq t \leq t' < w$ gilt und benutzen wir das Repräsentantensystem $0, \ldots, w-1$ modulo w, so läßt sich die Bedingung an die Parameter als $t' - t \geq ((l - l') \pmod w)$ schreiben. Die Inklusion überträgt sich natürlich auf die Bilder unter ϕ und somit erhalten wir

Bemerkung 2.14 *Benutzen wir das Repräsentantensystem* $0, \ldots, w-1$ *modulo* w *und ist* $t' - t \geq ((l - l') \pmod w)$*, so gilt:*
$(\mathcal{A}(w, l', t')|_{\operatorname{Kern}\phi})^{\perp\!\!\!\perp} \subseteq (\mathcal{A}(w, l, t)|_{\operatorname{Kern}\phi})^{\perp\!\!\!\perp}$,
$\phi(\mathcal{A}(w, l', t'))^{\perp\!\!\!\perp} \subseteq \phi(\mathcal{A}(w, l, t))^{\perp\!\!\!\perp}$,
$\mathcal{A}(w, l, t)|_{\operatorname{Kern}\phi} \subseteq \mathcal{A}(w, l', t')|_{\operatorname{Kern}\phi}$,
$\phi(\mathcal{A}(w, l, t)) \subseteq \phi(\mathcal{A}(w, l', t'))$.

2.3 Die Bestimmung von $\rho(\phi, w, l, t)$

Bemerkung 2.15 *Sei* $b_1, \ldots, b_u$ *eine Basis des Untervektorraums* $\mathbf{U} \subseteq \mathbb{F}_{q^r}$ *über* $\mathbb{F}_q$*. Sei* $l, k \in \mathbb{Z}$ *mit* $\operatorname{ggt}(k, r) = 1$*. Dann ist die Matrix* $M = (m_{i,j})$ *mit* $m_{i,j} = b_i^{q^{kj+l}}$ $1 \leq i, j \leq u$ *invertierbar.*

Beweis: Da Multiplikation mit Elementen aus $\mathbb{F}_{q^r}^\times$ und Potenzieren mit q Vektorraumautomorphismen sind, kann man durch Übergang zu $\tilde{b}_i := (b_i/b_1)^{q^l}$ ObdA annehmen, daß $b_1 = 1$ und $l = 0$ ist. Seien die Zahlen $a_{i,t}$ definiert durch $a_{i,1} := b_i$ und

$$a_{i,t} := \frac{a_{i,t-1}^{q^k} - a_{i,t-1}}{a_{t,t-1}^{q^k} - a_{t,t-1}} \quad \text{für } 2 \leq t \leq i \leq u.$$

Insbesondere ist $a_{t,t} = 1$. Definiere $M_t := (m_{i,j})$ mit $m_{i,j} := a_{i,t}^{q^{kj}}$

Behauptung:

i) Die $a_{i,t}$ $1 \leq t \leq i \leq u$ sind wohldefiniert.

ii) Für festes t sind die $a_{i,t}$ $t \leq i \leq u$ linear unabhängig über $\mathbb{F}_q$.

iii) $\det(M_{t-1}) = \det(M_t)(a_{t,t-1}^{q^k} - a_{t,t-1})^{\sum_{j=0}^{u-t} q^{kj}}$

Beweis durch Induktion nach t. Der Induktionsanfang $t = 1$ ist nach Voraussetzung erfüllt. Annahme die Behauptung gelte für $t - 1 \geq 1$. Als erstes müssen wir uns überlegen, welche Nullstellen $X^{q^k} - X$ in $\mathbb{F}_{q^r}$ hat. Dies sind offensichtlich die Elemente, die in $\mathbb{F}_{q^r} \cap \mathbb{F}_{q^k} = \mathbb{F}_{q^{\operatorname{ggt}(r,k)}}$ liegen. Nach Voraussetzung ist $\operatorname{ggt}(r, k) = 1$, also sind die Nullstellen von $X^{q^k} - X$ in $\mathbb{F}_{q^r}$ gerade die Elemente in $\mathbb{F}_q$.

i) Da nach Induktionsvoraussetzung $1 = a_{t-1,t-1}$ und $a_{t,t-1}$ linear unabhängig über $\mathbb{F}_q$ sind, liegt $a_{t,t-1}$ nicht in $\mathbb{F}_q$. Damit ist $a_{t,t-1}^{q^k} - a_{t,t-1} \neq 0$, also die $a_{i,t}$, $t \leq i \leq u$ wohldefiniert.

ii) Sei $\lambda_t, \ldots, \lambda_n \in \mathbb{F}_q$ mit $0 = \sum_{i=t}^{u} \lambda_i a_{i,t}$. So gilt:

$$\begin{aligned} 0 = & \sum_{i=t}^{u} \lambda_i a_{i,t} = \sum_{i=t}^{u} \lambda_i \frac{a_{i,t-1}^{q^k} - a_{i,t-1}}{a_{t,t-1}^{q^k} - a_{t,t-1}} \\ \Leftrightarrow \quad 0 = & \sum_{i=t}^{u} \lambda_i (a_{i,t-1}^{q^k} - a_{i,t-1}) = (\sum_{i=t}^{u} \lambda_i a_{i,t-1})^{q^k} - \sum_{i=t}^{u} \lambda_i a_{i,t-1} \\ \Leftrightarrow \quad & \sum_{i=t}^{u} \lambda_i a_{i,t-1} = \lambda_{t-1} \in \mathbb{F}_q \end{aligned}$$

Nach Induktionvoraussetzung sind die $a_{i,t-1}$, $t-1 \leq i \leq u$ linear unabhängig über $\mathbb{F}_q$, also $\lambda_{t-1} = \ldots = \lambda_n = 0$ und somit sind auch die $a_{i,t}$ $t \leq i \leq u$ linear unabhängig über $\mathbb{F}_q$.

iii)

$$\begin{aligned} |M_{t-1}| &= \begin{vmatrix} 1 & 1 & \ldots & 1 \\ a_{t,t-1} & a_{t,t-1}^{q^k} & \ldots & a_{t,t-1}^{q^{k(u-t+1)}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{u,t-1} & a_{u,t-1}^{q^k} & \ldots & a_{u,t-1}^{q^{k(u-t+1)}} \end{vmatrix} \\ &= \begin{vmatrix} 1 & 0 & \ldots & 0 \\ a_{t,t-1} & a_{t,t-1}^{q^k} - a_{t,t-1} & \ldots & (a_{t,t-1}^{q^k} - a_{t,t-1})^{q^{k(u-t)}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{u,t-1} & a_{u,t-1}^{q^k} - a_{u,t-1} & \ldots & (a_{u,t-1}^{q^k} - a_{u,t-1})^{q^{k(u-t)}} \end{vmatrix} \\ &= (a_{t,t-1}^{q^k} - a_{t,t-1})^{\sum_{j=0}^{u-t} q^{kj}} \, |M_t| \end{aligned}$$

Aus iii) erhalten wir rekursiv $\det(M) = \prod_{t=2}^{u} (a_{t,t-1}^{q^k} - a_{t,t-1})^{\sum_{j=0}^{u-t} q^{kj}}$. Wie in Punkt i) gesehen, ist $a_{t,t-1}^{q^k} - a_{t,t-1} \neq 0$ für alle $2 \leq t < u$ und damit $\det(M) \neq 0$ ■

Definiere für diesen Abschnitt $\mathbf{W} \subset \mathbb{F}_{q^r}$ die Gruppe der w-ten Einheitswurzeln.

Definition 2.16 $\mathrm{tr} = \mathrm{tr}_{F_{q^r}/F_q} : \mathbb{F}_{q^r} \longrightarrow \mathbb{F}_q$, $\mathrm{tr}(x) = \sum_{i=1}^{r} x^{q^i}$

$R \subset \mathbb{Z}$ sei ein Repräsentantensystem von $\mathbb{Z}/(w\mathbb{Z})$

$Z(j) := \{n \equiv jq^l \in R \,|\, 1 \leq l \leq r\}$ *die* zyklotomische Nebenklasse *von j.*

Sei $f = \sum_{i=1}^{t} a_i X^i$. $E(f) := \{n \in R \,|\, n \equiv i, a_i \neq 0\}$

$\mathcal{T}(j) := \{f \in \mathbb{F}_{q^r}[X]/(X^w - 1) \,|\, E(f) \subset Z(j)\}$

Satz 2.17 *Sei $s = |Z(j)|$ und $\mathrm{tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ die Spur. Für ein Polynom $f = \sum_{i=1}^{s}(a_i X^j)^{q^i} \in \mathcal{T}(j)$ gilt:*

$$\mathrm{tr}(f(w)) = 0 \quad \forall w \in \mathbf{W} \Leftrightarrow \sum_{i=1}^{s} a_i \in \mathrm{Kern}(\mathrm{tr}_{\mathbb{F}_{q^r}/\mathbb{F}_{q^s}})$$

Beweis: Ist $s = |Z(j)|$, so ist $\mathbb{F}_{q^s}$ der kleinste Körper für den $\mathbf{W}^j \subseteq \mathbb{F}_{q^s}$. Denn $s = |Z(j)|$ heißt, daß s die kleinste Zahl < 0 ist, so daß $jq^s \equiv j \pmod{w}$. Also $wl = j(q^s - 1)$ für ein $l \in \mathbb{N}$. Damit ist s die kleinste Zahl, so daß $(\mathbf{W}^j)^{q^s-1} = \mathbf{W}^{j(q^s-1)} = \mathbf{W}^{wl} = 1$, also $\mathbf{W}^j \subseteq \mathbb{F}_{q^s}$.

Definiere $\mathrm{tr} = \mathrm{tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}$, $\mathrm{Tr} = \mathrm{tr}_{\mathbb{F}_{q^r}/\mathbb{F}_{q^s}}$ und $\mathrm{tr}_s = \mathrm{tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$. Da $\mathrm{tr} = \mathrm{tr}_s \circ \mathrm{Tr}$ ist und nach obiger Überlegung $\mathbf{W}^j \subseteq \mathbb{F}_{q^s}$ ist, haben wir

$$\mathrm{tr}(\sum_{i=1}^{s} a_i^{q^i} x^{jq^i}) = \mathrm{tr}_s(\sum_{i=1}^{s} \mathrm{Tr}(a_i^{q^i} x^{jq^i})) = \mathrm{tr}_s(\sum_{i=1}^{s} \mathrm{Tr}(a_i)^{q^i} x^{jq^i})$$

für alle $x \in \mathbf{W}$. Denn die Potenzierung mit q kann man mit der Spur vertauschen, da q-Potenzierung ein Körperautomorphismus ist. Wir haben also das Problem die $\tilde{a}_i \in \mathbb{F}_{q^s}$ zu bestimmen, die $\mathrm{tr}_s(\sum_{i=1}^{s} \tilde{a}_i^{q^i} x^{jq^i}) = 0$ für alle $x \in \mathbf{W}$ erfüllen. Also:

$$\begin{aligned} 0 = \mathrm{tr}_s(\sum_{i=1}^{s} \tilde{a}_i^{q^i} x^{jq^i}) &= \sum_{k=1}^{s}(\sum_{i=1}^{s} \tilde{a}_i^{q^i} x^{jq^i}))^{q^k} \\ = \sum_{k=1}^{s}\sum_{i=1}^{s} \tilde{a}_i^{q^{i+k}} x^{jq^{i+k}} &= \sum_{l=1}^{s}(\sum_{i=1}^{s} \tilde{a}_i)^{q^l} x^{jq^l} \end{aligned}$$

Man erhält als hinreichende Bedingung $\sum_{i=1}^{s} \tilde{a}_i = 0$. Diese Bedingung ist auch notwendig, denn wir haben uns überlegt, daß $\mathbb{F}_{q^s}$ der kleinste Körper ist, für den $\mathbf{W}^j = \mathbf{W}^{jq^l} \subseteq \mathbb{F}_{q^s}$ ist. Also erzeugt $\mathbf{W}^{jq^l}$ $\mathbb{F}_{q^s}$ als Vektorraum. Seien $x_1, \ldots, x_s \in \mathbf{W}$, so daß $x_1^j, \ldots, x_s^j$ eine Basis von $\mathbb{F}_{q^s}$ ist. Dann ist, nach Bemerkung 2.15, die Determinante der Matrix $M = (m_{k,l})$ mit $m_{k,l} = x_k^{jq^l} \quad 1 \le k, l \le s$ ungleich Null. Also hat das Gleichungssystem $\sum_{l=1}^{s}(\sum_{i=1}^{s} \tilde{a}_i)^{q^l} x_k^{jq^l} = 0$ für $1 \le k \le s$ nur die Lösung $\sum_{i=1}^{s} \tilde{a}_i = 0$.

Man erhält daraus alle Lösungen des ursprünglichen Problems $\mathrm{tr}(\sum_{i=1}^{s} a_i^{q^i} x^{jq^i}) = 0$, indem man $a_i \in \mathrm{Tr}^{-1}(\tilde{a}_i)$ wählt. Da Tr eine surjektive Abbildung auf $\mathbb{F}_{q^s}$ist, bedeutet dies lediglich $a_i \in \mathbb{F}_{q^r}$. Die Bedingung $\sum_{i=1}^{s} \tilde{a}_i = 0$ transformiert sich durch Zurückziehen auf das Urbild, in $\sum_{i=1}^{s} a_i \in \mathrm{Kern}(\mathrm{Tr})$. ■

Definition 2.18 *Für einen Untervektorraum $\mathbf{U} \subseteq \mathbb{F}_{q^r}$ definiere:*
$\mathcal{P}(\mathbf{U}) := \{f \in \mathbb{F}_q[X]/(X^w - 1) \,|\, f(x) \in \mathbf{U} \quad \forall x \in \mathbf{W}\}$,
$\mathcal{T}(i, \mathbf{U}) := \mathcal{P}(\mathbf{U}) \cap \mathcal{T}(i)$.

Als nächstes werden wir bestimmen, wieviele Polynome vom Grad $\leq t$ es in $\mathcal{P}(\mathbf{U})$ gibt. Um vom Grad reden zu können, brauchen wir eine Anordnung der Restklassen der Exponenten. Diese legen wir durch die Wahl des Repräsentantensystems R von $\mathbb{Z}/(w\mathbb{Z})$ fest.

Definition 2.19 *Verwenden wir in R die durch $\mathbb{Z}$ gegebene Anordnung. Sei $f = \sum_{i\in R} a_i X^i \in \mathbb{F}_{q^n}[X]/(X^w - 1)$ mit $a_t \neq 0$ und für alle $i > t$ ist $a_i = 0$. So sagen wir f habe* Grad t.

Für gegebenes Repräsentantensystem R seien $\mathcal{P}(j, \mathbf{U})$ die Polynome vom Grad höchstens j in $\mathcal{P}(\mathbf{U})$. Diese bilden einen $\mathbb{F}_q$-Vektorraum mit $\dim_{\mathbb{F}_q} \mathcal{P}(j, \mathbf{U}) =: \rho(j)$. Jedes Polynom vom Grad j in $\mathcal{P}(j, \mathbf{U})$, läßt sich als Summe eines Polynoms aus $\mathcal{T}(j, \mathbf{U})$ vom Grad j und eines Polynoms aus $\mathcal{P}(j^-, \mathbf{U})$ schreiben, wobei j^- als der Vorgänger von j in der durch R gegebenen Anordnung definiert ist. Damit sehen wir, daß $\Delta\rho(j) := \rho(j) - \rho(j^-)$, die Dimension des Raums der Polynome vom Grad $\leq j$ in $\mathcal{T}(j, \mathbf{U})$ minus der Dimension des Raums der Polynome vom Grad $< j$ in $\mathcal{T}(j, \mathbf{U})$ ist.

Verwenden wir das Repräsentantensystem $R = \{l, \ldots, w+l-1\}$ und ist ϕ eine $\mathbb{F}_q$-lineare Abbildung mit $\mathrm{Kern}(\phi) = \mathbf{U}$, so ist das gesuchte $\rho(\phi, w, l, t) = \rho(l+t-1)$. Denn wir können jedes Polynom in $\mathcal{P}(l + t - 1, \mathbf{U})$ in der Form $X^l h(X)$ mit $Grad(h) < t$ schreiben, da nach Wahl des Repräsentantensystems keine Monome vom Grad kleiner als l vorkommen. Außerdem sind nach Definition die Polynome in $\mathcal{P}(\mathbf{U})$ gerade die, deren Werte für alle $x \in \mathbf{W}$, in $\mathrm{Kern}(\phi) = \mathbf{U}$ liegen. Damit haben wir gesehen:

Bemerkung 2.20 *Sei $R = \{l, \ldots, w+l-1\}$ und sei ϕ eine $\mathbb{F}_q$-lineare Abbildung mit* $\mathrm{Kern}(\phi) = \mathbf{U}$. *So ist $\Delta\rho(t + l - 1) := \rho(\phi, w, l, t) - \rho(\phi, w, l, t - 1)$, die Dimension des Raums der Polynome vom Grad $\leq l+t-1$ in $\mathcal{T}(l+t-1, \mathbf{U})$ minus der Dimension des Raums der Polynome vom Grad $< l+t-1$ in $\mathcal{T}(l+t-1, \mathbf{U})$.*

Betrachten wir also die Polynome in $\mathcal{T}(j, \mathbf{U})$ genauer. Dabei wird sich die Einführung der Spurform als nützlich erweisen.

Definition 2.21 *Sei* $\mathrm{tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ *die Spur. Definiere die* Spurform $\langle x, y\rangle_{\mathrm{tr}}$ *als* $\langle x, y\rangle_{\mathrm{tr}} := \mathrm{tr}(xy)$. *Ist $\mathbf{U}$ ein Untervektorraum von $\mathbb{F}_{q^r}$ über $\mathbb{F}_q$, so definiere* $\mathbf{U}^{\mathrm{tr}} := \{v \in \mathbb{F}_{q^r} \mid \mathrm{tr}(vu) = 0, \forall u \in \mathbf{U}\}$, *das orthogonale Komplement bezüglich der Spurform.*

Damit bekommen wir trivialerweise:

Bemerkung 2.22 *Sei $\mathbf{U}$ ein Untervektorraum der Dimension $r - u$ von $\mathbb{F}_{q^r}$.*

i) $\langle x, y\rangle_{\mathrm{tr}}$ *ist eine Bilinearform auf* $\mathbb{F}_{q^r}|\mathbb{F}_q$. $\mathbf{U}^{\mathrm{tr}}$ *ist ein Untervektorraum der Dimension* u *und es gilt* $(\mathbf{U}^{\mathrm{tr}})^{\mathrm{tr}} = \mathbf{U}$.

ii) Ist $\alpha_1, \ldots, \alpha_u$ *eine Basis von* $\mathbf{U}^{\mathrm{tr}}$, *so ist* $x \in \mathbf{U}$ *genau dann, wenn* $tr(\alpha_i x) = 0 \quad \forall 1 \leq i \leq u$

Damit bekommen wir folgende Charakterisierung der Polynome in $\mathcal{T}(j, \mathbf{U})$:

Satz 2.23 *Sei* $\mathrm{tr} := \mathrm{tr}_{F_{q^r}/F_q}$, $s = |Z(j)|$ *und* $\mathrm{Tr} := \mathrm{tr}_{F_{q^r}/F_{q^s}}$. *Sei* $\alpha_1, \ldots, \alpha_u$ *eine Basis von* $\mathbf{U}^{\mathrm{tr}}$. *So gilt:*

$$f = \sum_{i=1}^{s} (a_i X^j)^{q^i} \in \mathcal{T}(j, \mathbf{U}) \Leftrightarrow \sum_{i=1}^{s} \alpha_k^{q^{-i}} a_i \in \mathrm{Kern}(\mathrm{Tr}) \quad \forall 1 \leq k \leq u$$

Beweis: Nach Bemerkung 2.22 ist $f \in \mathcal{T}(j, \mathbf{U})$ äquivalent zu $\mathrm{tr}(\alpha_k f(w)) = 0 \quad \forall 1 \leq k \leq u, \forall w \in \mathbf{W}$. Nach Satz 2.17 ist dies wiederum äquivalent zu $\sum_{i=1}^{s} \alpha_k^{q^{-i}} a_i \in \mathrm{Kern}(\mathrm{Tr}) \, \forall 1 \leq k \leq u$ ■

Bemerkung 2.24 $\dim_{F_q}(\mathcal{T}(j, \mathbf{U})) = |Z(j)| \dim_{F_q}(\mathbf{U})$

Beweis: Sei $\alpha_1, \ldots, \alpha_u$ eine Basis von $\mathbf{U}^{\mathrm{tr}}$ und $M := (m_{i,j})$ mit $m_{i,j} := \alpha_i^{q^{-j}}$. Da die α_i eine Basis bilden, hat nach Bemerkung 2.15 M maximalen Rang: $\mathrm{Min}(u, |Z(j)|)$. Sei $s = |Z(j)|$, $\mathrm{Tr} = \mathrm{tr}_{F_{q^r}/F_{q^s}}$ und $\mathbf{K} := \mathrm{Kern}(\mathrm{Tr})$. Nach Satz 2.23 ist $\dim_{F_q}(\mathcal{T}(j, \mathbf{U}))$ die $\mathbb{F}_q$-Dimension des Lösungsraums des linearen Gleichungssystems $M\mathbf{x} \in \mathbf{K}^u$. Zuerst werden wir $\dim_{F_q}(\mathcal{T}(j, \mathbf{U})) \geq |Z(j)| \dim_{F_q}(\mathbf{U})$ zeigen.

Fall $u \leq s$: Da M maximalen Rang u hat, kann man also geeignete $s - u$ der x_i beliebig in $\mathbb{F}_{q^r}$ wählen und erhält dann die restlichen x_i, eindeutig durch Vorgabe einer rechten Seite $\mathbf{k}$. Dabei kann man $\mathbf{k}$ beliebig in $\mathbf{K}^u$ wählen. Also ist $\dim_{F_q}(\mathcal{T}(j, \mathbf{U})) = (s-u)r + (r-s)u = s(r-u) = |Z(j)| \dim_{F_q}(\mathbf{U})$.

Fall $u > s$: Weil M maximalen Rang, hier also s, hat, ist die $\mathbb{F}_q$-Dimension des von den Spalten von M erzeugten Raums $M\mathbb{F}_{q^r}^s$ gleich rs. Die zugelassenen rechten Seiten, $\mathbf{K}^u$ sind ebenfalls ein $\mathbb{F}_q$ Vektorraum. Dieser hat $\mathbb{F}_q$-Dimension $u(r-s)$. Gesucht ist die Dimension von deren Schnitt, $M\mathbb{F}_{q^r}^s \cap \mathbf{K}^u$. Es gilt die $\mathbb{F}_q$-Dimension des Erzeugnisses von $M\mathbb{F}_{q^r}^s$ und $\mathbf{K}^u$ ist

$$sr + u(r-s) - \dim_{F_q} M\mathbb{F}_{q^r}^s \cap \mathbf{K}^u \leq ru$$

der Dimension des ganzen Raums. Damit ist

$$\dim_{F_q}(M\mathbb{F}_{q^r}^s \cap \mathbf{K}^u) \geq sr + u(r-s) - ru = s(r-u) = |Z(j)| \dim(\mathbf{U}).$$

Nun wollen wir die Gleichheit zeigen. Dazu vergleichen wir mit der $\mathbb{F}_q$-Dimension von $\mathcal{P}(\mathbf{U})$. $\dim \mathcal{P}(\mathbf{U})$ ist $w \dim(\mathbf{U})$, denn nach Bemerkung 2.8 erhält man alle Polynome in $\mathcal{P}(\mathbf{U})$ gerade als die Polynome, bei denen man an (allen) w Stellen einen beliebigen Wert aus $\mathbf{U}$ vorschreibt. Sei Y ein Repräsentantensystem der $Z(j)$ (also $Y \subset \mathbb{Z}/(w)$ *s.d.* $|Y \cap Z(j)| = 1$ für alle $j \in \mathbb{Z}/(w)$). $\mathcal{P}(\mathbf{U})$ ist die disjunkte Vereinigung der $\mathcal{T}(j, \mathbf{U})$ für $j \in Y$. Ebenfalls klar ist, daß $w = \sum_{j \in Y} |Z(j)|$. Damit haben wir:

$$w \dim_{\mathbb{F}_q}(\mathbf{U}) = \dim_{\mathbb{F}_q} \mathcal{P}(\mathbf{U}) = \sum_{j \in Y} \dim_{\mathbb{F}_q} \mathcal{T}(j, \mathbf{U}) \geq \sum_{j \in Y} |Z(j)| \dim_{\mathbb{F}_q}(\mathbf{U}) = w \dim_{\mathbb{F}_q}(\mathbf{U}).$$

und somit muß $\dim_{\mathbb{F}_q}(\mathcal{T}(j, \mathbf{U})) = |Z(j)| \dim_{\mathbb{F}_q}(\mathbf{U})$ für alle j gelten ■

Nun weiter mit der Bestimmung von $\Delta\rho(j)$. Sei ein Repräsentantensystem R gegeben. Sei $s = |Z(j)|$ und seien $z_1 < \ldots < z_s$ die Elemente von $Z(j)$ in der durch R induzierten Anordnung. Schreibe $z_k = z_1 q^{\pi(k)}$, wobei π eine bijektive Abbildung von $\{1, \ldots, s\}$ auf $\{0, \ldots, s-1\}$ ist. Definiere die Matrix $M = M(Z(j))$ als $M = (m_{i,k})$ mit $m_{i,k} = \alpha_i^{q^{-\pi(k)}} \quad 1 \leq i \leq u, 1 \leq k \leq s$. Sei $S_i \subseteq \mathbb{F}_{q^r}^u$ der von den ersten i Spalten von M über $\mathbb{F}_{q^r}$ erzeugte Vektorraum. Sei desweiteren $\mathbf{K} = \operatorname{Kern} \operatorname{tr}_{\mathbb{F}_{q^r}/\mathbb{F}_{q^s}}$. Definiere die $\mathbb{F}_q$-Dimension $d_i := \dim(S_i \cap \mathbf{K}^u)$.

Sei $j = z_i$ und M_i die Matrix M eingeschränkt auf die ersten i Spalten. Aus der Charakterisierung durch Satz 2.23 sehen wir, daß die $\mathbb{F}_q$-Dimension des Raums der Polynome vom Grad $\leq j$ in $\mathcal{T}(j, \mathbf{U})$, gerade die $\mathbb{F}_q$-Dimension des Lösungsraums des Gleichungssystems $M_i \mathbf{x} \in \mathbf{K}^u$ ist. Diese ist $ri - (\dim_{\mathbb{F}_q}(S_i) - d_i)$. Sei $j = l + t - 1$, so bekommt man durch Bemerkung 2.20

$$\Delta\rho(j) = \rho(\phi, w, l, t) - \rho(\phi, w, l, t-1) = r + (d_i - d_{i-1}) - (\dim(S_i) - \dim(S_{i-1}))$$

Dies läßt sich weiter vereinfachen. Laut Bemerkung 2.15 folgt, daß M maximalen Rang $\kappa = \operatorname{Min}(u, s)$ hat. Sei $H := \{h_1, \ldots, h_\kappa\}$, $1 \leq h_1 \leq \ldots \leq h_\kappa \leq s$ die Zahlen für die $\operatorname{rang}(M_{h_i}) = 1 + \operatorname{rang}(M_{h_i - 1})$. Klarerweise ist $h_1 = 1$. Damit gilt für $h \in H$, daß $\dim(S_h) - \dim(S_{h-1}) = r$. Für $h \notin H$ dagegen ist $\dim(S_h) = \dim(S_{h-1})$ und $d_h = d_{h-1}$.

Betrachten wir noch zwei Spezialfälle. Im Fall $|Z(j)| = r$ ist $\mathbf{K} = \mathbf{0}$ und somit $d_i = 0$ für alle i. Im Fall $|Z(j)| = 1$ ist $d_1 = \dim_{\mathbb{F}_q}(\mathcal{T}(j, \mathbf{U}))$ und somit nach Bemerkung 2.24 $d_1 = \dim_{\mathbb{F}_q}(\mathbf{U}) = r - u$.

Damit bekommen wir nun den eigentlichen Satz für die Bestimmung von ρ:

Satz 2.25 *Sei w ein Teiler von $q^r - 1$. Sei ϕ eine $\mathbb{F}_q$-lineare Abbildung mit $\operatorname{Kern}(\phi) = \mathbf{U}$ und $\alpha_1, \ldots, \alpha_u$ eine Basis von $\mathbf{U}^{\mathrm{tr}}$. Sei $j := l + t - 1$, $Z = Z(j)$ die zyklotomische Nebenklasse von j und $s = |Z|$. Wählen wir $R = l, \ldots, l + w - 1$ als Repräsentantensystem von $\mathbb{Z}/(w)$. Seien $z_1 < \ldots < z_s$ die Elemente von $Z(j)$ in*

der durch R induzierten Anordnung. Schreibe $z_k = z_1 q^{\pi(k)}$ wobei π eine bijektive Abbildung von $\{1, \ldots, s\}$ auf $\{0, \ldots, s-1\}$ ist. Definiere die Matrix $M = M(Z)$ als $M = (m_{i,k})$ mit $m_{i,k} = \alpha_i^{q^{-\pi(k)}}$ $1 \leq i \leq u$, $1 \leq k \leq s$. Sei $S_i \subseteq \mathbb{F}_{q^r}^u$ der von den ersten i Spalten von M über $\mathbb{F}_{q^r}$ erzeugte Vektorraum. Sei desweiteren $\mathrm{Tr} = \mathrm{tr}_{F_{q^r}/F_{q^s}}$ *und* $\mathbf{K} = \mathrm{Kern}\,\mathrm{Tr}$. *Definiere die $\mathbb{F}_q$-Dimension $d_i := \dim(S_i \cap \mathbf{K}^u)$. Sei $\kappa = \mathrm{Min}(u, s)$ und $H = \{1 = h_1 < \ldots < h_\kappa\}$ die Menge der Indizes h für die $\dim(S_h) > \dim(S_{h-1})$ ist. Ist $j = z_i$ und setze $d_0 = 0$, so gilt:*

$$\Delta\rho(j) = \rho(\phi, w, l, t) - \rho(\phi, w, l, t-1) = \begin{cases} r & \text{falls } i \notin H, \\ d_i - d_{i-1} & \text{falls } i \in H \end{cases}$$

Dabei gibt es noch folgende Spezialfälle:

$$\Delta\rho(j) = \begin{cases} 0 & \text{falls } i \in H,\ s = r, \\ r - u & \text{falls } i \in H,\ s = 1 \end{cases}$$

Bemerkung 2.26 (Die Bestimmung von d_1) *Sei $Z = Z(j)$ mit $s = |Z|$ und* $\mathrm{Kern}(\phi) = \mathbf{U}$. *Sei* $\mathrm{tr} = \mathrm{tr}_{F_{q^r}/F_q}$. *Sei d die $\mathbb{F}_{q^s}$-Dimension des von $\mathbf{U}^{\mathrm{tr}}$ über $\mathbb{F}_{q^s}$ erzeugten Unterraums. So ist $d_1 = r - ds$.*

Beweis: Sei $\alpha_1, \ldots, \alpha_u$ eine Basis von U^{tr}, $\mathrm{Tr} = \mathrm{tr}_{F_{q^r}/F_{q^s}}$ und $\mathbf{K} = \mathrm{Kern}(\mathrm{Tr})$. Nach Definition ist $d_1 = \dim(S_1 \cap \mathbf{K}^u)$, also ist d_1 die Dimension des Raums $\mathbf{V} = \{x \in \mathbb{F}_{q^r} \,|\alpha_k x \in \mathbf{K}, \forall 1 \leq i \leq u\}$. Sei $\tilde{\mathbf{U}}$ der von $\alpha_1, \ldots, \alpha_u$ über $\mathbb{F}_{q^s}$ erzeugte Unterraum, so ist $\mathbf{V} = \tilde{\mathbf{U}}^{\mathrm{Tr}}$. Sei $d := \dim_{F_{q^s}}(\tilde{\mathbf{U}})$. Damit ist $\dim_{F_{q^s}}(\mathbf{V}) = r/s - d$. Beachtet man noch, daß der von $\alpha_1, \ldots, \alpha_u$ und der von U^{tr} über $\mathbb{F}_{q^s}$ erzeugte Unterraum derselbe ist, so folgt die Behauptung. (Somit ist $\mathbf{V} = (\mathbf{U}^{\mathrm{tr}})^{\mathrm{Tr}}$) ■

Bemerkung 2.27 (Die Bestimmung von h_2) *Sei $Z = Z(j)$ mit $s = |Z| > 1$ und π wie oben definiert. Sei* $\mathrm{Kern}(\phi) = \mathbf{U}$. *Sei* $\mathrm{tr} = \mathrm{tr}_{F_{q^r}/F_q}$. *Sei $\alpha \in \mathbf{U}^{\mathrm{tr}} \backslash \{0\}$ und k minimal mit der Eigenschaft $\alpha^{-1}\mathbf{U}^{\mathrm{tr}} \subseteq \mathbb{F}_{q^k}$. So ist h_2 das Minimum der Zahlen $i > 1$, so daß k nicht $\pi(i)$ teilt.*

Ist in obiger Bemerkung $k = r$, so ist immer $h_2 = 2$, also das zugehörige Element das zweitkleinste der zyklotomischen Nebenklasse $Z(j)$.

Beweis: Nach Bemerkung 2.12 kann man ObdA annehmen $1 \in \mathbf{U}^{\mathrm{tr}}$. Somit sagt die Voraussetzung der Bemerkung, daß $\mathbf{U}^{\mathrm{tr}} \subseteq \mathbb{F}_{q^k}$. Nach Definition ist h_2 Minimum der Zahlen $i > 1$, so daß die Spalten $(\alpha_1, \ldots, \alpha_u)^t$ und $(\alpha_1^{q^{-\pi(i)}}, \ldots, \alpha_u^{q^{-\pi(i)}})^t$ linear unabhängig über $\mathbb{F}_{q^r}$ sind. Aus Satz 2.15 folgt die Behauptung ■

Sei $\mathrm{ggt}(u, r) = s$ und ist $\mathbf{U}^{\mathrm{tr}}$ sogar ein u/s-dimensionaler $\mathbb{F}_{q^s}$-Vektorraum, so ist auch $\mathbf{U}$ ein $\mathbb{F}_{q^s}$-Vektorraum. Man kann also als $\mathbb{F}_q$-lineare Abbildung ϕ, mit

Kern(ϕ) = $\mathbf{U}$, sogar eine $\mathbb{F}_{q^s}$-lineare Abbildung ϕ benutzen. Da es bei der Bestimmung von ρ nur auf den Kern von ϕ ankommt, bekommen wir also dieselben Parameter wie im entsprechenden $\mathbb{F}_{q^s}$-linearen Fall für $\tilde{u} = u/s$. Zu beachten ist nur, daß die vorkommenden Dimensionen sich um den Faktor s unterscheiden, da man in einem Fall $\mathbb{F}_q$-Dimensionen im anderen $\mathbb{F}_{q^s}$-Dimensionen betrachtet.

Da die zyklotomische Nebenklasse von 0 nur aus 0 besteht, ist es egal, ob man die Anordnung bezüglich des Repräsentantensystems $0, \ldots, w-1$, oder bezüglich $1, \ldots, w$ betrachtet. Man erhält für beide Wahlen dasselbe $\Delta\rho(j)$. Beachten wir, daß $\Delta\rho(0) = r - u$ ist, so sehen wir, daß $\rho(\phi, w, 1, t) + r - u = \rho(\phi, w, 0, t+1)$ für alle $t < w$ ist. Ist $\phi(\mathcal{A}(w, 1, t))^{\perp\!\!\!\perp}$ ein $\mathbb{F}_q$-linearer, q^u-ärer $[w, k, t+1]$, so folgt aus obiger Überlegung, daß $\phi(\mathcal{A}(w, 0, t+1))^{\perp\!\!\!\perp}$ ein $[w, k-u, t+2]$ ist. Außerdem gilt nach Bemerkung 2.14, daß $[w, k, t+1] \supset [w, k-u, t+2]$ ist. Konstruktion X mit dem trivialen $\mathbb{F}_q$-linearen, q^u-ären $[1, u, 1]$ (dem q^u-ären, linearen $[1, 1, 1]$) liefert einen $[w+1, k, t+2]$. Dieser wird im Fall $u = 1$ (BCH-Codes) der erweiterte BCH-Code genannt. Wir bekommen also:

Bemerkung 2.28 *Ist $\mathcal{C} = \phi(\mathcal{A}(w, 1, t))^{\perp\!\!\!\perp}$ ein $\mathbb{F}_q$-linearer, q^u-ärer $[w, k, t+1]$, so existiert der erweiterte Code $\hat{\mathcal{C}}$ mit den Parametern $[w+1, k, t+2]$*

Besonders einfach gestaltet sich die Bestimmung von $\rho(\phi, w, l, t) - \rho(\phi, w, l, t-1)$ in den Fällen $u = 1, 2$:

2.3.1 Der Fall $u = 1$ (BCH-Codes)

In diesem Fall gibt es nur ein h_i, nämlich $h_1 = 1$. Das zugehörige Element ist nach Definition das kleinste Element der zyklotomischen Nebenklasse $Z(t)$.

Definition 2.29 *Wählen wir $R = l, \ldots, l+w-1$ als Repräsentantensystem von $\mathbb{Z}/(w)$. j heiße* minimal, *falls $j \leq i \quad \forall i \in Z(j)$, in der durch R induzierten Anordnung.*

Damit bekommen wir:

Satz 2.30 *Sei w ein Teiler von $q^r - 1$. Sei ϕ eine $\mathbb{F}_q$-lineare Abbildung von $\mathbb{F}_{q^r}$ mit eindimensionalem Bild. Wählen wir $R = l, \ldots, l + w - 1$ als Repräsentantensystem von $\mathbb{Z}/(w)$, so ist:*

$$\rho(\phi, w, l, t) - \rho(\phi, w, l, t-1) = \begin{cases} r - |Z(t+l-1)| & \text{falls } t+l-1 \text{ minimal} \\ r & \text{sonst} \end{cases}$$

Beweis: Nach Bemerkung 2.26 ist $d_1 = r - |Z(j)|$. Damit folgt die Behauptung aus Satz 2.25 ■

2.3.2 Der Fall $u = 2$

Satz 2.31 *Sei w ein Teiler von $q^r - 1$. Sei ϕ eine $\mathbb{F}_q$-lineare Abbildung von $\mathbb{F}_{q^r}$ mit zweidimensionalem Bild und* $\mathrm{Kern}(\phi) = \mathbf{U}$. *Sei α_1, α_2, eine Basis von $\mathbf{U}^{\mathrm{tr}}$. Sei $\mathbb{F}_{q^k}$ der von α_1/α_2 erzeugte Teilkörper von $\mathbb{F}_{q^r}$. Setze $j := l + t - 1$. Wählen wir $R = l, \ldots, l + w - 1$ als Repräsentantensystem von $\mathbb{Z}/(w)$. Sei $s = |Z(j)|$ und seien $z_1 < \ldots < z_s$ die Elemente von $Z(j)$ in der durch R induzierten Anordnung. Sei $z_i = z_1^{q^{-\pi(i)}}$. Sei h_2 die minimale Zahl > 1, so daß k nicht $\pi(h_2)$ teilt. Ist $j = z_i$, so gilt:*

- *Falls $k|s$:* $\rho(\phi, w, l, t) - \rho(\phi, w, l, t-1) = \begin{cases} r - s & \text{falls } i \in \{1, h_2\} \\ r & \text{sonst} \end{cases}$
- *Falls $k \nmid s$:* $\rho(\phi, w, l, t) - \rho(\phi, w, l, t-1) = \begin{cases} r - 2s & \text{falls } i = 1 \\ r & \text{sonst} \end{cases}$

Beweis: d_1 und h_2 sind gemäß Bemerkung 2.26 bzw. 2.27 gewählt. Wir wissen, daß $\Delta\rho(j+1)$ für alle $i \notin \{1, h_2\}$ gleich r ist. Ist $s \geq 2$, so liefert Bemerkung 2.24, daß $(r-2)s = d_1 + d_2 + (s-2)r$. Also ist $d_2 = 2(r-s) - d_1$. Satz 2.25 liefert jetzt die Behauptung ■

2.3.3 Ein Beispiel

Als Beispiel wollen wir für $q = 2$, $w = 63$, $u = 2$ und $l = 1$ die Parameter der Codes $\phi(\mathcal{A}(w, l, t))^{\perp\!\!\!\perp}$ für verschiedene ϕ berechnen. Dazu notieren wir uns zuerst für $q = 2$ die zyklotomischen Nebenklassen modulo 63 für das Repräsentantensystem $1, \ldots, 63$. Die Einträge der Nebenklassen sind $z_1, 2 \cdot z_1, 4 \cdot z_1, \ldots$.

$Z(j)$
1,2,4,8,16,32
3,6,12,24,48,33
5,10,20,40,17,34
7,14,28,56,49,35
9,18,36
11,22,44,25,50,37
13,26,52,41,19,38
15,30,60,57,51,39
21,42
23,46,29,58,53,43
27,54,45
31,62,61,59,55,47
63

Satz 2.31 zeigt uns, daß es drei verschiedene Klassen von ϕ gibt, die durch den Grad k des Teilkörpers bestimmt sind, der von α_1/α_2 erzeugt wird. Hierbei ist α_1, α_2, eine Basis von $\mathrm{Kern}(\phi)^{\mathrm{tr}}$.

Im Fall $k = 6$ sind wir für $|Z(j)| < 6$ immer im "$k \nmid s$-Fall" von Satz 2.31. Außerdem gilt immer $h_2 = 2$, wie wir uns schon in der Anmerkung zu Bemerkung 2.27 überlegt haben. Wir bekommen durch Satz 2.31 also $\Delta\rho(t) = 0$ für $1 \leq t \leq 3$, da diese t die kleinsten bzw. zweitkleinsten Elemente ihrer Nebenklasse sind. $\Delta\rho(4) = 6$, da 4 das drittkleinste Element der zyklotomischen Nebenklasse $Z(1) = Z(4)$ ist. Für $5 \leq t \leq 7$ haben wir wieder $\Delta\rho(t) = 0$, für $t = 8$ ist $\Delta\rho(8) = 6$. Für $t = 9$ ist $3 = s = |Z(9)|$. Wir sind im Fall $k \nmid s$, also ist auch hier $\Delta\rho(9) = 0$. Es ist klar wie es weitergeht. Man überlege sich vielleicht noch, daß $\Delta\rho(18) = 6$ und $\Delta\rho(21) = 2$ ist.

Im Fall $k = 3$ läuft alles wie im Fall $k = 6$ bis $t = 8$. Für $t = 9$ sind wir hier im $k|s$-Fall, deshalb ist hier $\Delta\rho(9) = \Delta\rho(18) = 3$. Auch hier tritt der Fall $h_2 \neq 2$ nie ein, denn sonst müßte $\pi(h_2) = 3$ sein, also das zweitkleinste Element der zyklotomischen Nebenklasse das kleinste mal q^3 modulo w. Das hieße das zweitkleinste Element stünde in der vierten Spalte in obiger Tabelle. Man überzeugt sich leicht davon, daß dies nie der Fall ist.

Der Fall $k = 2$ entspricht dem Fall für $q = 4$ und $u = 1$, wie wir uns überlegt haben. Er ist trotzdem interessant, da hier der Fall $h_2 \neq 2$ auftritt. Mit derselben Überlegung wie im Fall $k = 3$ sehen wir, daß der Fall $h_2 \neq 2$ eintritt wenn das zweitkleinste Element der zyklotomischen Nebenklasse in der dritten oder fünften Spalte in obiger Tabelle steht. Dies tritt für $t = 19, 29, 45$ ein. Wir haben in all diesen Fällen $h_2 = 3$.

Nach Lemma 2.11 ist die Dimension von $\phi(\mathcal{A}(63, 1, t))^{\perp\!\!\!\perp}$ gleich $2 \cdot 63 - 6 \cdot t + \rho(\phi, 63, 1, t)$. Berechnen wir alle $\Delta\rho(t)$, so erhalten wir folgende Codes:

	$k=6$		$k=3$		$k=2$	
t	$\rho(t)$	$\phi_k(\mathcal{A})^{\perp\!\!\!\perp}$	$\rho(t)$	$\phi_k(\mathcal{A})^{\perp\!\!\!\perp}$	$\rho(t)$	$\phi_k(\mathcal{A})^{\perp\!\!\!\perp}$
1	0	$[63, 120, 2]$	0	$[63, 120, 2]$	0	$[63, 120, 2]$
2	0	$[63, 114, 3]$	0	$[63, 114, 3]$	0	$[63, 114, 3]$
3	0	$[63, 108, 4]$	0	$[63, 108, 4]$	0	$[63, 108, 5]$
4	6	$[63, 108, 5]$	6	$[63, 108, 5]$	6	$[63, 108, 5]$
5	6	$[63, 102, 6]$	6	$[63, 102, 6]$	6	$[63, 102, 6]$
6	6	$[63, 96, 7]$	6	$[63, 96, 7]$	6	$[63, 96, 7]$
7	6	$[63, 90, 8]$	6	$[63, 90, 8]$	6	$[63, 90, 8]$
8	12	$[63, 90, 9]$	12	$[63, 90, 9]$	12	$[63, 90, 9]$
9	12	$[63, 84, 10]$	15	$[63, 87, 10]$	12	$[63, 84, 10]$
10	12	$[63, 78, 11]$	15	$[63, 81, 11]$	12	$[63, 78, 11]$
11	12	$[63, 72, 12]$	15	$[63, 75, 12]$	12	$[63, 72, 12]$
12	18	$[63, 72, 13]$	21	$[63, 75, 13]$	18	$[63, 72, 13]$
13	18	$[63, 66, 14]$	21	$[63, 69, 14]$	18	$[63, 66, 14]$
14	18	$[63, 60, 15]$	21	$[63, 63, 15]$	18	$[63, 60, 15]$
15	18	$[63, 54, 16]$	21	$[63, 57, 16]$	18	$[63, 54, 16]$
16	24	$[63, 54, 17]$	27	$[63, 57, 17]$	24	$[63, 54, 17]$
17	30	$[63, 54, 18]$	33	$[63, 57, 18]$	30	$[63, 54, 18]$
18	36	$[63, 54, 19]$	36	$[63, 54, 19]$	36	$[63, 54, 19]$
19	36	$[63, 48, 20]$	36	$[63, 48, 20]$	42	$[63, 54, 20]$
20	42	$[63, 48, 21]$	42	$[63, 48, 21]$	48	$[63, 54, 21]$
21	44	$[63, 44, 22]$	44	$[63, 44, 22]$	52	$[63, 52, 22]$
22	44	$[63, 38, 23]$	44	$[63, 38, 23]$	52	$[63, 46, 23]$
23	44	$[63, 32, 24]$	44	$[63, 32, 24]$	52	$[63, 40, 24]$
24	50	$[63, 32, 25]$	50	$[63, 32, 25]$	58	$[63, 40, 25]$
25	56	$[63, 32, 26]$	56	$[63, 32, 26]$	64	$[63, 40, 26]$
26	62	$[63, 32, 27]$	62	$[63, 32, 27]$	64	$[63, 34, 27]$
27	62	$[63, 26, 28]$	65	$[63, 29, 28]$	64	$[63, 28, 28]$
28	68	$[63, 26, 29]$	71	$[63, 29, 29]$	70	$[63, 28, 29]$
29	68	$[63, 20, 30]$	71	$[63, 23, 30]$	76	$[63, 28, 30]$
30	68	$[63, 14, 31]$	71	$[63, 17, 31]$	76	$[63, 22, 31]$
31	68	$[63, 8, 32]$	71	$[63, 11, 32]$	76	$[63, 16, 32]$
41	128	$[63, 8, 42]$	131	$[63, 11, 42]$	136	$[63, 16, 42]$
42	134	$[63, 8, 43]$	137	$[63, 11, 43]$	140	$[63, 14, 43]$
43	140	$[63, 8, 44]$	143	$[63, 11, 44]$	140	$[63, 8, 44]$
44	146	$[63, 8, 45]$	149	$[63, 11, 45]$	146	$[63, 8, 45]$
45	152	$[63, 8, 46]$	152	$[63, 8, 46]$	152	$[63, 8, 46]$
46	158	$[63, 8, 47]$	158	$[63, 8, 47]$	158	$[63, 8, 47]$
47	158	$[63, 2, 48]$	158	$[63, 2, 48]$	158	$[63, 2, 48]$
62	248	$[63, 2, 63]$	248	$[63, 2, 63]$	248	$[63, 2, 63]$

Dabei entsprechen wie gesagt die Parameter im Fall $k = 2$ dem quaternären, linearen Code, nur daß es sich in obiger Tabelle um $\mathbb{F}_2$-Dimensionen handelt, so daß man noch durch 2 dividieren muß, um zu $\mathbb{F}_4$-Dimensionen, wie im quaternären, linearen üblich, zu gelangen. Einfacher erhält man die Parameter in diesem Fall natürlich durch Satz 2.30. In den Intervallen $32 \leq t \leq 40$ und $48 \leq t \leq 61$, die in der Tabelle fehlen, steigt $\rho(t)$ immer um 6 und die Dimension des Codes bleibt konstant.

3 Konstruktion neuer Codes aus BCH-Codes

In diesem Abschnitt wollen wir unsere Kenntnisse der BCH-Codes dazu benutzen neue Codes zu konstruieren. Sei ζ eine w-te Einheitswurzel in $\mathbb{F}_{q^r}$. Wir benutzen die durch Satz 2.13 gelieferte Identifizierung des q-ären BCH-Codes mit den Nullstellen $\zeta^l, \ldots, \zeta^{l+t-1}$, mit $\phi(\mathcal{A}(w,l,t))^{\perp\!\!\!\perp}$. Wie wir im Beweis von Satz 2.13 gesehen haben, können wir als $\mathbb{F}_q$-lineare Abbildung ϕ ObdA die Spur $\mathrm{tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ benutzen. Zur Vereinfachung definieren wir folgende Notation:

Definition 3.1 $\mathcal{B}(w,l,t) := \mathcal{B}(l,t) := \mathrm{tr}(\mathcal{A}(w,l,t))^{\perp\!\!\!\perp}$, *wobei wir w weglassen wenn dessen Wert aus dem Zusammenhang hervorgeht. Die Dimension von $\mathcal{B}(w,l,t)$ sei $k(w,l,t) = k(l,t)$. Damit hat $\mathcal{B}(w,l,t)$ die Parameter $[w, k(l,t), t+1]$.*

Nach Lemma 2.11 ist $k(w,l,t)$, die Dimension des BCH-Codes, wie folgt bestimmt:

$$k(w,l,t) = w - rt + \rho(\mathrm{tr}, w, l, t)$$

wobei sich die ρ's einfach rekursiv aus Satz 2.30 bestimmen lassen.

Für $q = 4$ ist $\mathcal{B}(65,22,22)$ ein $[65,27,23]$, dieser ist neu.

3.1 Konstruktion X

Als erste wollen wir Konstruktion X (Bemerkung 1.17) auf BCH-Codes anwenden. Für Konstruktion X benötigen wir einen Code mit einem Teilcode höherer Distanz. Seien

$$\bar{\mathcal{C}} = \mathcal{B}(w,l,t) \quad \text{und} \quad \mathcal{C}' = \mathcal{B}(w,l',t')$$

Nach Bemerkung 2.14 gilt $\bar{\mathcal{C}} \supseteq \mathcal{C}'$, falls $t' - t \geq ((l - l') \mod w)$ ist (wobei wir $0, \ldots, w-1$ als Vertretersystem modulo w benutzen).

Trivialerweise gibt es dann auch für jedes k mit $k(l,t) \geq k > k(l',t')$ einen linearen Code $\mathcal{C}$ der Dimension k mit $\bar{\mathcal{C}} \supseteq \mathcal{C} \supseteq \mathcal{C}'$ (Basisergänzung). Damit ist $\mathcal{C}$ also ein $[w,k,t+1]$. Gibt es einen linearen, q-ären Hilfscode $[n, k-k(l',t'), \delta]$ mit $\delta \leq t' - t$, so garantiert Konstruktion X die Existenz eines $[w+n, k, t+1+\delta]$. Damit haben wir folgende Konstruktion für neue Codes.

Satz 3.2 *Sei w ein Teiler von $q^r - 1$. Benutzen wir $0, \ldots, w-1$ als Vertretersystem modulo w und sei $t' - t \geq ((l - l') \mod w)$. Sei $k \in \mathbb{N}$, so daß $k(l,t) \geq k > k(l',t')$. Gibt es einen linearen, q-ären Hilfscode $\mathcal{D}$ $[n, k-k(l',t'), \delta]$ mit $\delta \leq t' - t$. So gibt es einen linearen, q-ären Code $\mathcal{E}$ mit den Parametern $[w+n, k, t+1+\delta]$.*

Als Anwendung von Satz 3.2 erhalten wir mit den obigen Bezeichnungen folgende Tabellen neuer Codes. Wobei wir das verwendete k aus der Dimension von $\mathcal{E}$ ablesen können.

3.1.1 $q = 2$

$\mathcal{E}$	$\bar{\mathcal{C}}$	(l,t)	$\mathcal{C}'$	(l',t')	$\mathcal{D}$
$[264, 215, 13]$	$[255, 215, 11]$	$(1, 10)$	$[255, 207, 13]$	$(1, 12)$	$[9, 8, 2]$
$[264, 199, 17]$	$[255, 199, 15]$	$(1, 14)$	$[255, 191, 17]$	$(1, 16)$	$[9, 8, 2]$
$[259, 135, 34]$	$[255, 142, 30]$	$(239, 29)$	$[255, 134, 34]$	$(239, 33)$	$[4, 1, 4]$
$[260, 134, 36]$	$[255, 134, 34]$	$(239, 33)$	$[255, 130, 36]$	$(237, 35)$	$[5, 4, 2]$
$[143, 34, 39]$	$[127, 36, 31]$	$(1, 30)$	$[127, 29, 43]$	$(1, 42)$	$[16, 5, 8]$
$[142, 31, 41]$	$[127, 36, 31]$	$(1, 30)$	$[127, 29, 43]$	$(1, 42)$	$[15, 2, 10]$
$[148, 34, 41]$	$[127, 36, 31]$	$(1, 30)$	$[127, 29, 43]$	$(1, 42)$	$[21, 5, 10]$
$[151, 36, 41]$	$[127, 36, 31]$	$(1, 30)$	$[127, 29, 43]$	$(1, 42)$	$[24, 7, 10]$
$[139, 30, 43]$	$[127, 36, 31]$	$(1, 30)$	$[127, 29, 43]$	$(1, 42)$	$[12, 1, 12]$
$[145, 31, 43]$	$[127, 36, 31]$	$(1, 30)$	$[127, 29, 43]$	$(1, 42)$	$[18, 2, 12]$
$[151, 34, 43]$	$[127, 36, 31]$	$(1, 30)$	$[127, 29, 43]$	$(1, 42)$	$[24, 5, 12]$
$[154, 36, 43]$	$[127, 36, 31]$	$(1, 30)$	$[127, 29, 43]$	$(1, 42)$	$[27, 7, 12]$
$[131, 23, 47]$	$[127, 29, 43]$	$(1, 42)$	$[127, 22, 47]$	$(1, 46)$	$[4, 1, 4]$
$[135, 26, 47]$	$[127, 29, 43]$	$(1, 42)$	$[127, 22, 47]$	$(1, 46)$	$[8, 4, 4]$
$[136, 17, 53]$	$[127, 22, 47]$	$(1, 46)$	$[127, 15, 55]$	$(1, 54)$	$[9, 2, 6]$
$[139, 19, 53]$	$[127, 22, 47]$	$(1, 46)$	$[127, 15, 55]$	$(1, 54)$	$[12, 4, 6]$
$[159, 28, 53]$	$[127, 29, 43]$	$(1, 42)$	$[127, 15, 55]$	$(1, 54)$	$[32, 13, 10]$
$[161, 29, 53]$	$[127, 29, 43]$	$(1, 42)$	$[127, 15, 55]$	$(1, 54)$	$[34, 14, 10]$
$[139, 17, 55]$	$[127, 22, 47]$	$(1, 46)$	$[127, 15, 55]$	$(1, 54)$	$[12, 2, 8]$
$[161, 27, 55]$	$[127, 29, 43]$	$(1, 42)$	$[127, 15, 55]$	$(1, 54)$	$[34, 12, 12]$
$[164, 29, 55]$	$[127, 29, 43]$	$(1, 42)$	$[127, 15, 55]$	$(1, 54)$	$[37, 14, 12]$
$[154, 8, 75]$	$[127, 8, 63]$	$(1, 62)$	$[127, 1, 127]$	$(1, 126)$	$[27, 7, 12]$
$[167, 8, 81]$	$[127, 8, 63]$	$(1, 62)$	$[127, 1, 127]$	$(1, 126)$	$[40, 7, 18]$
$[170, 8, 83]$	$[127, 8, 63]$	$(1, 62)$	$[127, 1, 127]$	$(1, 126)$	$[43, 7, 20]$
$[174, 8, 85]$	$[127, 8, 63]$	$(1, 62)$	$[127, 1, 127]$	$(1, 126)$	$[47, 7, 22]$
$[177, 8, 87]$	$[127, 8, 63]$	$(1, 62)$	$[127, 1, 127]$	$(1, 126)$	$[50, 7, 24]$
$[264, 45, 89]$	$[255, 45, 87]$	$(1, 86)$	$[255, 37, 91]$	$(1, 90)$	$[9, 8, 2]$
$[258, 38, 92]$	$[255, 38, 90]$	$(171, 89)$	$[255, 36, 92]$	$(169, 91)$	$[3, 2, 2]$
$[258, 30, 96]$	$[255, 30, 94]$	$(171, 93)$	$[255, 28, 96]$	$(169, 95)$	$[3, 2, 2]$
$[258, 22, 104]$	$[255, 22, 102]$	$(171, 101)$	$[255, 20, 104]$	$(169, 103)$	$[3, 2, 2]$
$[261, 10, 126]$	$[255, 10, 122]$	$(171, 121)$	$[255, 8, 128]$	$(165, 127)$	$[6, 2, 4]$

3.1.2 $q = 3$

$\mathcal{E}$	$\bar{\mathcal{C}}$	(l,t)	$\mathcal{C}'$	(l',t')	$\mathcal{D}$
$[126,101,9]$	$[121,101,8]$	$(56,7)$	$[121,96,9]$	$(56,7)$	$[5,5,1]$
$[126,91,12]$	$[121,91,11]$	$(53,10)$	$[121,86,12]$	$(52,11)$	$[5,5,1]$
$[30,7,16]$	$[26,7,14]$	$(1,13)$	$[26,4,17]$	$(1,16)$	$[4,3,2]$
$[127,76,18]$	$[121,76,16]$	$(46,15)$	$[121,71,18]$	$(44,17)$	$[6,5,2]$
$[85,39,19]$	$[80,39,17]$	$(31,16)$	$[80,35,20]$	$(31,19)$	$[5,4,2]$
$[127,71,20]$	$[121,71,18]$	$(44,17)$	$[121,66,21]$	$(41,20)$	$[6,5,2]$
$[82,35,21]$	$[80,35,20]$	$(31,19)$	$[80,33,21]$	$(30,20)$	$[2,2,1]$
$[125,68,21]$	$[121,71,18]$	$(44,17)$	$[121,66,21]$	$(41,20)$	$[4,2,3]$
$[129,71,21]$	$[121,71,18]$	$(44,17)$	$[121,66,21]$	$(41,20)$	$[8,5,3]$
$[127,66,23]$	$[121,66,21]$	$(41,20)$	$[121,61,23]$	$(41,22)$	$[6,5,2]$
$[131,36,41]$	$[121,36,36]$	$(41,35)$	$[121,31,41]$	$(41,40)$	$[10,5,5]$
$[123,16,63]$	$[121,16,61]$	$(61,60)$	$[121,15,63]$	$(61,62)$	$[2,1,2]$
$[127,15,65]$	$[121,15,63]$	$(61,62)$	$[121,10,69]$	$(55,68)$	$[6,5,2]$
$[123,11,69]$	$[121,11,67]$	$(55,66)$	$[121,10,69]$	$(55,68)$	$[2,1,2]$
$[132,15,69]$	$[121,15,63]$	$(61,62)$	$[121,10,69]$	$(55,68)$	$[11,5,6]$

3.1.3 $q = 4$

$\mathcal{E}$	$\bar{\mathcal{C}}$	(l,t)	$\mathcal{C}'$	(l',t')	$\mathcal{D}$
$[90,67,10]$	$[85,67,8]$	$(29,7)$	$[85,63,10]$	$(27,9)$	[5,4,2]
$[89,63,11]$	$[85,63,10]$	$(27,9)$	$[85,59,11]$	$(26,10)$	$[4,4,1]$
$[72,46,12]$	$[65,46,10]$	$(61,9)$	$[65,40,12]$	$(60,11)$	$[7,6,2]$
$[72,27,25]$	$[65,27,23]$	$(22,22)$	$[65,21,25]$	$(21,24)$	$[7,6,2]$
$[84,27,29]$	$[65,27,23]$	$(22,22)$	$[65,15,31]$	$(18,30)$	$[19,12,6]$
$[87,27,31]$	$[85,27,29]$	$(57,28)$	$[85,26,31]$	$(57,30)$	$[2,1,2]$
$[77,8,50]$	$[65,8,44]$	$(44,43)$	$[65,2,52]$	$(40,51)$	$[12,6,6]$
$[95,6,66]$	$[85,6,60]$	$(56,59)$	$[85,2,68]$	$(52,67)$	$[10,4,6]$

3.2 Iterierte Konstruktion X

Seien $\mathcal{C} \supseteq \mathcal{C}' \supseteq \mathcal{C}''$ lineare, q-äre Codes mit den Parametern $[w,k,d]$, $[w,k',d']$ bzw. $[w,k'',d'']$. Wenden wir Konstruktion X mit dem Hilfscode $\mathcal{D}$, einem $[n,k-k',\delta]$, auf das Paar $\mathcal{C}$,$\mathcal{C}'$ an, so erhalten wir einen $[w+n,k,Min(d+\delta,d')]$. Dieser enthält $\mathcal{C}''$ als Teilcode. Wenden wir auf dieses Paar wiederum Konstruktion X mit Hilfscode $\mathcal{D}'$, einem $[n',k-k'',\delta']$, an, so erhalten wir einen Code $\mathcal{E}$ mit den Parametern $[w+n+n',k,Min(d+\delta+\delta',d'+\delta',d'')]$.

Verwenden wir in obiger Überlegung $\bar{\mathcal{C}} = \mathcal{B}(l,t)$, $\mathcal{C}' = \mathcal{B}(l',t')$ und $\mathcal{C}'' = \mathcal{B}(l'',t'')$. Nach Bemerkung 2.14 gilt $\bar{\mathcal{C}} \supseteq \mathcal{C}'$, falls $t'-t \geq ((l-l') \mod w)$ ist und $\mathcal{C}' \supseteq \mathcal{C}''$,

falls $t'' - t' \geq ((l' - l'') \mod w)$ ist (wobei wir $0, \ldots, w-1$ als Vertretersystem modulo w benutzen). Sei für $k \in \mathbb{N}$, mit $k(l,t) \geq k > k(l',t')$, $\mathcal{C}$ ein Code der Dimension k, so daß $\bar{\mathcal{C}} \supseteq \mathcal{C} \supseteq \mathcal{C}'$ gilt. Somit ist $\mathcal{C}$ ein $[w, k, t+1]$. Damit erhalten wir folgende Konstruktion:

Satz 3.3 *Sei w ein Teiler von $q^r - 1$. Benutzen wir $0, \ldots, w-1$ als Vertretersystem modulo w und sei $t' - t \geq ((l - l') \mod w)$, sowie $t'' - t' \geq ((l' - l'') \mod w)$. Sei $k \in \mathbb{N}$, so daß $k(l,t) \geq k > k(l',t')$ gilt. Gibt es lineare, q-äre Hilfscodes $\mathcal{D}$ und $\mathcal{D}'$ mit Parametern $[n, k - k(l',t'), \delta]$ bzw. $[n', k - k(l'',t''), \delta']$. So gibt es einen linearen, q-ären Code $\mathcal{E}$ mit den Parametern*

$$[w + n + n', k, 1 + Min(t + \delta + \delta', t' + \delta', t'')].$$

Man kann natürlich obige Konstruktion auf beliebig lange Ketten von Codes erweitern, aber in den von uns betrachteten Fällen bekommt man dadurch keine Codes, die man nicht auch durch eine der anderen Konstruktionen erhält.

Mit den obigen Bezeichnungen bekommt man folgende neue Codes. Hier kann man das verwendete k aus der Dimension von $\mathcal{E}$ ablesen.

3.2.1 $q = 2$

$\mathcal{E}$	w	$l, t, k(l,t)$	$l', t', k(l',t')$	$l'', t'', k(l'',t'')$	$\mathcal{D}$	$\mathcal{D}'$
$[142, 79, 19]$	127	$1, 12, 85$	$1, 14, 78$	$1, 18, 71$	$[2, 1, 2]$	$[13, 8, 4]$
$[144, 80, 19]$	127	$1, 12, 85$	$1, 14, 78$	$1, 18, 71$	$[3, 2, 2]$	$[14, 9, 4]$
$[146, 81, 19]$	127	$1, 12, 85$	$1, 14, 78$	$1, 18, 71$	$[4, 3, 2]$	$[15, 10, 4]$
$[142, 58, 27]$	127	$1, 20, 64$	$1, 22, 57$	$1, 26, 50$	$[2, 1, 2]$	$[13, 8, 4]$
$[144, 59, 27]$	127	$1, 20, 64$	$1, 22, 57$	$1, 26, 50$	$[3, 2, 2]$	$[14, 9, 4]$
$[146, 60, 27]$	127	$1, 20, 64$	$1, 22, 57$	$1, 26, 50$	$[4, 3, 2]$	$[15, 10, 4]$
$[89, 18, 31]$	63	$1, 20, 18$	$1, 22, 16$	$1, 30, 7$	$[3, 2, 2]$	$[23, 11, 8]$
$[148, 23, 53]$	127	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$[4, 1, 4]$	$[17, 8, 6]$
$[151, 24, 53]$	127	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$[6, 2, 4]$	$[18, 9, 6]$
$[153, 25, 53]$	127	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$[4, 3, 2]$	$[22, 10, 8]$
$[155, 26, 53]$	127	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$[5, 4, 2]$	$[23, 11, 8]$
$[157, 27, 53]$	127	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$[6, 5, 2]$	$[24, 12, 8]$
$[151, 23, 55]$	127	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$[4, 1, 4]$	$[20, 8, 8]$

$\mathcal{E}$	w	$l,t,k(l,t)$	$l',t',k(l',t')$	$l'',t'',k(l'',t'')$	$\mathcal{D}$	$\mathcal{D}'$
$[154,24,55]$	127	$1,42,29$	$1,46,22$	$1,54,15$	$[6,2,4]$	$[21,9,8]$
$[156,25,55]$	127	$1,42,29$	$1,46,22$	$1,54,15$	$[7,3,4]$	$[22,10,8]$
$[158,26,55]$	127	$1,42,29$	$1,46,22$	$1,54,15$	$[8,4,4]$	$[23,11,8]$
$[152,16,61]$	127	$1,46,22$	$1,54,15$	$1,62,8$	$[8,1,8]$	$[17,8,6]$
$[160,18,61]$	127	$1,46,22$	$1,54,15$	$1,62,8$	$[11,3,6]$	$[22,10,8]$
$[162,19,61]$	127	$1,46,22$	$1,54,15$	$1,62,8$	$[12,4,6]$	$[23,11,8]$
$[155,16,63]$	127	$1,46,22$	$1,54,15$	$1,62,8$	$[8,1,8]$	$[20,8,8]$
$[163,18,63]$	127	$1,46,22$	$1,54,15$	$1,62,8$	$[14,3,8]$	$[22,10,8]$

3.2.2 $q = 3$

$\mathcal{E}$	w	$l,t,k(l,t)$	$l',t',k(l',t')$	$l'',t'',k(l'',t'')$	$\mathcal{D}$	$\mathcal{D}'$
$[92,7,57]$	80	$31,49,7$	$31,50,6$	$31,59,2$	$[1,1,1]$	$[11,5,6]$

3.3 Konstruktion XX

Als nächstes wollen wir Konstruktion XX (Bemerkung 1.18) auf BCH-Codes anwenden. Wir benötigen dazu einen Code $\mathcal{C}$ mit Teilcodes $\mathcal{C}_1, \mathcal{C}_2$ und $\mathcal{C}' := \mathcal{C}_1 \cap \mathcal{C}_2$. Seien

$$\mathcal{C}' = \mathcal{B}(l',t') \quad \tilde{\mathcal{C}}_1 = \mathcal{B}(l',t'-i) \quad \tilde{\mathcal{C}}_2 = \mathcal{B}(l'+j,t'-j) \quad \tilde{\mathcal{C}} = \mathcal{B}(l,t)$$

Man überlegt sich leicht, daß der Schnitt zweier zyklischer Codes $\tilde{\mathcal{C}}_1$ und $\tilde{\mathcal{C}}_2$, gerade der zyklische Code ist, der sowohl die Nullstellen von $\tilde{\mathcal{C}}_1$ als auch von $\tilde{\mathcal{C}}_2$ hat. Nach Satz 2.13 ist $\tilde{\mathcal{C}}_i$ der zyklische Code mit den Nullstellen ζ^k, $k \in \{l', \ldots, l'+t'-i-1\}$ bzw. $k \in \{l'+j, \ldots, l'+t'-1\}$. Wählen wir $i,j \in \{0, \ldots, t'\}$, so daß $l'+t'-i-1 \geq l'+j$ also $t' \geq j+i+1$ ist, so bildet die Vereinigung der Nullstellen wieder ein Intervall, nämlich ζ^k $k \in \{l', \ldots, l'+t'-1\}$. Somit ist $\mathcal{C}' = \mathcal{B}(l',t') = \tilde{\mathcal{C}}_1 \cap \tilde{\mathcal{C}}_2$. Damit $\tilde{\mathcal{C}}_1, \tilde{\mathcal{C}}_2 \subseteq \tilde{\mathcal{C}}$ gilt, müssen wir nach Bemerkung 2.14 fordern: $l \geq l'+j$ und $l+t \leq l'+t'-i$.

Man beachte, daß die wahre designte Distanz von $\mathcal{C}'$ größer als $t'+1$ sein kann, auch wenn die Distanz der $\tilde{\mathcal{C}}_i$ und von $\tilde{\mathcal{C}}$ maximal sind. Dies tritt dann ein wenn, $\rho(tr,w,l'-1,t'+1) - \rho(tr,w,l',t') = r$ oder $\rho(tr,w,l',t'+1) - \rho(tr,w,l',t') = r$ ist. Sei $\mathcal{C}' = \mathcal{B}(l',t') = \mathcal{B}(\tilde{l}',\tilde{t}')$, wobei $\tilde{t}'+1$ die maximale Distanz von $\mathcal{C}'$ ist. Zu jeden k_1, k_2 und k in den Intervallen $k(l',t'-i) \geq k_1 > k(l',t')$, $k(l-j',t'-j) \geq k_2 > k(l',t')$ und $k(l,t) \geq k > k_1+k_2-k(l',t')$, existieren Codes $\mathcal{C}_1, \mathcal{C}_2$ und $\mathcal{C}$ der Dimension k_1, k_2 bzw k, für die $\tilde{\mathcal{C}} \supseteq \mathcal{C} \supset \tilde{\mathcal{C}}_i \supseteq \mathcal{C}_i$ und $\mathcal{C}_1 \cap \mathcal{C}_2 = \mathcal{C}'$ gilt. Existieren Hilfscode $\mathcal{D}_1$ bzw. $\mathcal{D}_2$ mit den Parametern $[n_1, k-k_1, \delta_1]$ bzw. $[n_2, k-k_2, \delta_2]$, so liefert Konstruktion XX einen

$$[w+n_1+n_2, k, 1+Min(t+\delta_1+\delta_2, t'-i+\delta_2, t'-j+\delta_1, \tilde{t}')].$$

Wir fassen dies in einem Satz zusammen:

Satz 3.4 *Sei w ein Teiler von $q^r - 1$. Gibt es zu $1 \leq t' \leq w$ und $1 \leq l' \leq w$ natürliche Zahlen i, j mit $i, j \in \{0, \ldots, t'\}$, so daß $t' \geq j + i + 1$. Sei $l \geq l' + j$ und $l + t \leq l' + t' - i$. Sei $\tilde{t}' + 1$ die maximale Distanz von $\mathcal{C}' = \mathcal{B}(l', t')$. Definiere $\tilde{k}_1 := k(l', t' - i)$ und $\tilde{k}_2 := k(l + j, t - j)$. Seien $k_1, k_2, k \in \mathbb{N}$ in den Intervallen $\tilde{k}_1 \geq k_1 > k(l', t')$, $\tilde{k}_2 \geq k_2 > k(l', t')$ und $k(l, t) \geq k > k_1 + k_2 - k(l', t')$ gegeben. Gibt es lineare Hilfscodes $\mathcal{D}_1$ bzw. $\mathcal{D}_2$ mit Parametern $[n_1, k - k_1, \delta_1]$ bzw. $[n_2, k - k_2, \delta_2]$. So gibt es einen Code $\mathcal{E}$ mit den Parametern*

$$[w + n_1 + n_2, k, 1 + Min(t + \delta_1 + \delta_2, t' - i + \delta_2, t' - j + \delta_1, \tilde{t}')].$$

Mit den Bezeichnungen des Satzes erhalten wir folgende Tabelle neuer Codes. Dabei erhält man k aus den Parametern von $\mathcal{E}$ und damit kann man k_1 und k_2 aus den Dimensionen von $\mathcal{D}_1$ und $\mathcal{D}_2$ berechnen. In den meisten Fällen stimmen sie aber mit $\tilde{k}_1$ und $\tilde{k}_2$ überein.

3.3.1 $q = 2$

$w = 63$

$\mathcal{E}$	$l, t, k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l', t', k(l', t')$	$(\tilde{l}', \tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[75, 39, 13]$	$55, 8, 39$	3	36	2	32	$53, 13, 29$	$(53, 13)$	$[4, 3, 2]$	$[8, 7, 2]$

$w = 127$

$\mathcal{E}$	$l, t, k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l', t', k(l', t')$	$(\tilde{l}', \tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[148, 78, 21]$	$1, 14, 78$	2	70	1	71	$125, 21, 63$	$(125, 21)$	$[9, 8, 2]$	$[12, 7, 4]$
$[144, 71, 23]$	$1, 18, 71$	2	63	3	64	$125, 23, 56$	$(125, 23)$	$[9, 8, 2]$	$[8, 7, 2]$
$[148, 57, 29]$	$1, 22, 57$	4	49	3	50	$125, 29, 42$	$(125, 29)$	$[9, 8, 2]$	$[12, 7, 4]$
$[158, 33, 45]$	$97, 31, 35$	2	28	12	28	$85, 45, 21$	$(85, 47)$	$[24, 5, 12]$	$[7, 7, 1]$
$[162, 35, 46]$	$97, 31, 35$	2	28	12	28	$85, 45, 21$	$(85, 47)$	$[27, 7, 12]$	$[8, 7, 2]$
$[142, 25, 49]$	$85, 43, 28$	4	21	4	21	$81, 51, 14$	$(81, 51)$	$[8, 7, 2]$	$[7, 4, 3]$
$[148, 29, 49]$	$85, 42, 29$	5	22	4	21	$81, 51, 14$	$(81, 51)$	$[12, 7, 4]$	$[9, 8, 2]$
$[147, 28, 50]$	$85, 43, 28$	4	21	4	21	$81, 51, 14$	$(81, 51)$	$[8, 7, 2]$	$[12, 7, 4]$
$[146, 25, 51]$	$85, 43, 28$	4	21	4	21	$81, 51, 14$	$(81, 51)$	$[12, 7, 4]$	$[7, 4, 3]$
$[152, 29, 51]$	$85, 42, 29$	5	22	4	21	$81, 51, 14$	$(81, 51)$	$[12, 7, 4]$	$[13, 8, 4]$
$[151, 28, 52]$	$85, 43, 28$	4	21	4	21	$81, 51, 14$	$(81, 51)$	$[12, 7, 4]$	$[12, 7, 4]$
$[150, 19, 57]$	$81, 47, 21$	4	14	8	14	$73, 59, 7$	$(73, 63)$	$[16, 5, 8]$	$[7, 7, 1]$
$[155, 22, 57]$	$81, 46, 22$	5	15	8	14	$73, 59, 7$	$(73, 63)$	$[19, 7, 8]$	$[9, 8, 2]$
$[173, 29, 57]$	$85, 42, 29$	5	15	12	21	$73, 59, 7$	$(73, 63)$	$[37, 14, 12]$	$[9, 8, 2]$
$[154, 21, 58]$	$81, 47, 21$	4	14	8	14	$73, 59, 7$	$(73, 63)$	$[19, 7, 8]$	$[8, 7, 2]$
$[172, 28, 58]$	$85, 43, 28$	4	14	12	21	$73, 59, 7$	$(73, 63)$	$[37, 14, 12]$	$[8, 7, 2]$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[154,19,59]$	$81,47,21$	4	14	8	14	$73,59,7$	$(73,63)$	$[16,5,8]$	$[11,7,3]$
$[157,21,59]$	$81,47,21$	4	14	8	14	$73,59,7$	$(73,63)$	$[18,7,7]$	$[12,7,4]$
$[159,22,59]$	$81,46,22$	5	15	8	14	$73,59,7$	$(73,63)$	$[19,7,8]$	$[13,8,4]$
$[177,29,59]$	$85,42,29$	5	15	12	21	$73,59,7$	$(73,63)$	$[37,14,12]$	$[13,8,4]$
$[165,21,61]$	$81,47,21$	7	14	8	14	$73,59,7$	$(73,63)$	$[23,7,9]$	$[15,7,5]$
$[167,22,61]$	$81,46,22$	5	15	8	14	$73,59,7$	$(73,63)$	$[23,7,9]$	$[17,8,6]$
$[155,15,65]$	$73,54,15$	9	8	8	7	$65,71,0$	$(65,127)$	$[19,7,8]$	$[9,8,2]$
$[154,14,66]$	$73,55,14$	8	7	8	7	$65,71,0$	$(65,127)$	$[8,7,2]$	$[19,7,8]$
$[157,14,67]$	$73,55,14$	8	7	8	7	$65,71,0$	$(65,127)$	$[11,7,3]$	$[19,7,8]$
$[159,15,67]$	$73,54,15$	9	8	8	7	$65,71,0$	$(65,127)$	$[12,7,4]$	$[20,8,8]$
$[161,14,69]$	$73,55,14$	8	7	8	7	$65,71,0$	$(65,127)$	$[15,7,5]$	$[19,7,8]$
$[163,15,69]$	$73,54,15$	9	8	8	7	$65,71,0$	$(65,127)$	$[16,7,6]$	$[20,8,8]$
$[164,14,71]$	$73,55,14$	8	7	8	7	$65,71,0$	$(65,127)$	$[18,7,7]$	$[19,7,8]$
$[166,15,71]$	$73,54,15$	9	8	8	7	$65,71,0$	$(65,127)$	$[19,7,8]$	$[20,8,8]$

$w = 255$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[265,223,12]$	$1,8,223$	2	222	1	215	$0,11,214$	$(0,11)$	$[1,1,1]$	$[9,8,2]$
$[273,230,12]$	$249,7,230$	2	222	2	222	$247,11,214$	$(247,11)$	$[9,8,2]$	$[9,8,2]$
$[286,238,12]$	$251,5,238$	2	222	4	230	$247,11,214$	$(247,11)$	$[22,16,4]$	$[9,8,2]$
$[265,207,16]$	$1,12,207$	2	206	1	199	$0,15,198$	$(0,15)$	$[1,1,1]$	$[9,8,2]$
$[273,214,16]$	$245,11,214$	2	206	2	206	$243,15,198$	$(243,15)$	$[9,8,2]$	$[9,8,2]$
$[280,217,16]$	$247,9,222$	2	206	4	214	$243,15,198$	$(243,15)$	$[16,11,4]$	$[9,8,2]$
$[286,222,16]$	$247,9,222$	2	206	4	214	$243,15,198$	$(243,15)$	$[22,16,4]$	$[9,8,2]$
$[261,191,20]$	$1,16,191$	2	190	1	187	$0,19,186$	$(0,19)$	$[1,1,1]$	$[5,4,2]$
$[272,198,20]$	$1,14,199$	4	198	1	187	$0,19,186$	$(0,19)$	$[1,1,1]$	$[16,11,4]$
$[274,199,20]$	$1,14,199$	4	198	1	187	$0,19,186$	$(0,19)$	$[1,1,1]$	$[18,12,4]$
$[265,187,22]$	$1,18,187$	2	186	1	179	$0,21,178$	$(0,21)$	$[1,1,1]$	$[9,8,2]$
$[269,190,22]$	$239,17,190$	2	186	2	182	$237,21,178$	$(237,21)$	$[5,4,2]$	$[9,8,2]$
$[280,197,22]$	$241,15,198$	2	186	4	190	$237,21,178$	$(237,21)$	$[16,11,4]$	$[9,8,2]$
$[265,179,24]$	$1,20,179$	2	178	1	171	$0,23,170$	$(0,23)$	$[1,1,1]$	$[9,8,2]$
$[273,186,24]$	$237,19,186$	2	178	2	178	$235,23,170$	$(235,23)$	$[9,8,2]$	$[9,8,2]$
$[280,189,24]$	$239,17,190$	2	178	4	182	$235,23,170$	$(235,23)$	$[16,11,4]$	$[9,8,2]$
$[265,171,26]$	$1,22,171$	2	170	1	163	$0,25,162$	$(0,25)$	$[1,1,1]$	$[9,8,2]$
$[273,178,26]$	$235,21,178$	2	170	2	170	$233,25,162$	$(233,25)$	$[9,8,2]$	$[9,8,2]$
$[280,181,26]$	$237,19,186$	2	170	4	178	$233,25,162$	$(233,25)$	$[16,11,4]$	$[9,8,2]$
$[265,163,28]$	$1,24,163$	2	162	1	155	$0,27,154$	$(0,27)$	$[1,1,1]$	$[9,8,2]$
$[273,170,28]$	$233,23,170$	2	162	2	162	$231,27,154$	$(231,27)$	$[9,8,2]$	$[9,8,2]$
$[280,173,28]$	$235,21,178$	2	162	2	170	$231,27,154$	$(231,27)$	$[16,11,4]$	$[9,8,2]$
$[265,155,30]$	$1,26,155$	2	154	1	147	$0,29,146$	$(0,29)$	$[1,1,1]$	$[9,8,2]$
$[273,162,30]$	$231,25,162$	2	154	2	154	$229,29,146$	$(229,29)$	$[9,8,2]$	$[9,8,2]$
$[280,165,30]$	$233,23,170$	2	154	4	162	$229,29,146$	$(229,29)$	$[16,11,4]$	$[9,8,2]$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[265,147,32]$	$1,28,147$	2	146	1	139	$0,31,138$	$(0,31)$	$[1,1,1]$	$[9,8,2]$
$[273,154,32]$	$229,27,154$	2	146	2	146	$227,31,138$	$(227,31)$	$[9,8,2]$	$[9,8,2]$
$[265,131,40]$	$1,36,131$	2	130	1	132	$0,39,122$	$(0,39)$	$[1,1,1]$	$[9,8,2]$
$[265,115,46]$	$1,42,115$	2	114	1	107	$0,45,106$	$(0,45)$	$[1,1,1]$	$[9,8,2]$
$[272,118,46]$	$217,39,122$	2	114	2	114	$213,45,106$	$(213,45)$	$[8,4,4]$	$[9,8,2]$
$[277,122,46]$	$217,39,122$	2	114	4	114	$213,45,106$	$(213,45)$	$[13,8,4]$	$[9,8,2]$
$[265,107,48]$	$1,44,107$	2	106	1	99	$0,47,98$	$(0,47)$	$[1,1,1]$	$[9,8,2]$
$[273,114,48]$	$213,43,114$	2	106	2	106	$211,47,98$	$(211,47)$	$[9,8,2]$	$[9,8,2]$
$[261,91,54]$	$1,50,91$	2	90	1	87	$0,53,86$	$(0,53)$	$[1,1,1]$	$[9,8,2]$
$[265,87,56]$	$1,52,87$	2	86	1	79	$0,55,78$	$(0,55)$	$[1,1,1]$	$[9,8,2]$
$[269,90,56]$	$205,51,90$	2	86	2	82	$203,55,78$	$(203,55)$	$[5,4,2]$	$[9,8,2]$
$[259,47,88]$	$1,84,47$	2	46	1	45	$0,87,44$	$(0,87)$	$[1,1,1]$	$[9,8,2]$

3.3.2 $q = 3$

$w = 56$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[58,10,30]$	$1,27,10$	1	9	1	9	$0,29,8$	$(0,29)$	$[1,1,1]$	$[1,1,1]$

$w = 80$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[90,71,8]$	$39,3,71$	2	67	2	67	$37,7,63$	$(37,7)$	$[5,4,2]$	$[5,4,2]$
$[85,64,9]$	$1,6,64$	1	63	1	60	$0,8,59$	$(0,8)$	$[1,1,1]$	$[4,4,1]$
$[89,67,9]$	$36,5,67$	1	63	2	63	$34,8,59$	$(34,8)$	$[5,4,2]$	$[4,4,1]$
$[91,68,9]$	$36,4,68$	2	64	2	63	$34,8,59$	$(34,8)$	$[5,4,2]$	$[6,5,2]$
$[88,63,10]$	$34,7,63$	1	59	1	59	$33,9,55$	$(33,9)$	$[4,4,1]$	$[4,4,1]$
$[86,60,11]$	$1,7,60$	1	59	1	56	$0,10,55$	$(0,10)$	$[1,1,1]$	$[5,4,2]$
$[90,63,11]$	$36,6,63$	2	59	2	59	$34,10,55$	$(34,10)$	$[5,4,2]$	$[5,4,2]$
$[83,56,12]$	$1,9,56$	1	55	1	54	$0,11,53$	$(0,11)$	$[1,1,1]$	$[2,2,1]$
$[90,60,12]$	$1,7,60$	3	59	1	54	$0,11,53$	$(0,11)$	$[1,1,1]$	$[9,6,3]$
$[86,55,13]$	$31,10,55$	1	53	1	51	$30,12,49$	$(30,12)$	$[2,2,1]$	$[4,4,1]$
$[88,56,13]$	$1,9,56$	3	55	1	50	$0,13,49$	$(0,13)$	$[1,1,1]$	$[7,6,2]$
$[93,59,13]$	$33,8,59$	1	53	3	55	$30,12,49$	$(30,12)$	$[9,6,3]$	$[4,4,1]$
$[95,60,13]$	$33,7,60$	2	54	3	55	$30,12,49$	$(30,12)$	$[9,6,3]$	$[6,5,2]$
$[86,54,14]$	$1,10,54$	2	53	1	50	$0,13,49$	$(0,13)$	$[1,1,1]$	$[5,4,2]$
$[90,56,14]$	$1,9,56$	3	55	1	50	$0,13,49$	$(0,13)$	$[1,1,1]$	$[9,6,3]$
$[85,50,15]$	$1,12,50$	1	49	1	46	$0,14,45$	$(0,14)$	$[1,1,1]$	$[4,4,1]$
$[89,53,15]$	$30,11,53$	1	49	2	49	$28,14,45$	$(28,14)$	$[5,4,2]$	$[4,4,1]$
$[91,54,15]$	$30,10,55$	2	50	2	49	$28,14,45$	$(28,14)$	$[5,4,2]$	$[6,5,2]$
$[93,55,15]$	$31,10,55$	1	49	3	51	$28,14,45$	$(28,14)$	$[9,6,3]$	$[4,4,1]$
$[95,56,15]$	$31,9,56$	2	50	3	51	$28,14,45$	$(28,14)$	$[9,6,3]$	$[6,5,2]$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[88,49,16]$	$28,13,49$	1	45	1	45	$27,15,41$	$(27,15)$	$[4,4,1]$	$[4,4,1]$
$[90,50,16]$	$1,12,50$	3	49	1	42	$0,16,41$	$(0,16)$	$[1,1,1]$	$[9,8,2]$
$[94,53,16]$	$30,11,53$	3	49	2	45	$28,16,41$	$(28,16)$	$[5,4,2]$	$[9,8,2]$
$[86,46,17]$	$1,13,46$	2	45	1	42	$0,16,41$	$(0,16)$	$[1,1,1]$	$[5,4,2]$
$[90,49,17]$	$30,12,49$	2	45	2	45	$28,16,41$	$(28,16)$	$[5,4,2]$	$[5,4,2]$
$[92,50,17]$	$1,12,50$	3	49	1	42	$0,16,41$	$(0,16)$	$[1,1,1]$	$[11,8,3]$
$[96,53,17]$	$30,11,53$	3	49	2	45	$28,16,41$	$(28,16)$	$[5,4,2]$	$[11,8,3]$
$[100,55,17]$	$31,10,55$	3	49	3	47	$28,16,41$	$(28,16)$	$[9,6,3]$	$[11,8,3]$
$[89,45,18]$	$27,14,45$	1	41	2	41	$25,17,37$	$(25,17)$	$[5,4,2]$	$[4,4,1]$
$[88,41,19]$	$25,16,41$	1	37	1	37	$24,18,33$	$(24,18)$	$[4,4,1]$	$[4,4,1]$
$[86,37,21]$	$31,16,39$	3	37	1	35	$30,20,33$	$(30,20)$	$[2,2,1]$	$[4,2,3]$
$[89,39,21]$	$31,16,39$	3	37	1	35	$30,20,33$	$(30,20)$	$[2,2,1]$	$[7,4,3]$
$[84,35,22]$	$31,19,35$	1	33	1	33	$30,21,31$	$(30,21)$	$[2,2,1]$	$[2,2,1]$
$[84,34,23]$	$1,19,34$	2	33	1	32	$0,22,31$	$(0,22)$	$[1,1,1]$	$[3,2,2]$
$[92,38,23]$	$1,16,38$	5	37	1	32	$0,22,31$	$(0,22)$	$[1,1,1]$	$[11,6,5]$
$[85,32,24]$	$1,21,32$	1	31	1	28	$0,23,27$	$(0,23)$	$[1,1,1]$	$[4,4,1]$
$[87,33,24]$	$21,20,33$	1	31	2	29	$19,23,27$	$(19,23)$	$[3,2,2]$	$[4,4,1]$
$[89,34,24]$	$21,19,34$	2	32	2	29	$19,23,27$	$(19,23)$	$[3,2,2]$	$[6,5,2]$
$[88,31,25]$	$19,22,31$	1	27	1	27	$18,24,23$	$(18,24)$	$[4,4,1]$	$[4,4,1]$
$[109,24,41]$	$1,24,24$	15	23	1	16	$0,40,15$	$(0,40)$	$[1,1,1]$	$[28,8,15]$
$[86,15,44]$	$1,40,15$	3	14	1	11	$0,44,10$	$(0,44)$	$[1,1,1]$	$[5,4,2]$
$[85,13,45]$	$1,40,15$	3	14	1	11	$0,44,10$	$(0,44)$	$[1,1,1]$	$[4,2,3]$
$[88,15,45]$	$1,40,15$	3	14	1	11	$0,44,10$	$(0,44)$	$[1,1,1]$	$[7,4,3]$
$[90,16,45]$	$1,39,16$	4	15	1	11	$0,44,10$	$(0,44)$	$[1,1,1]$	$[9,5,4]$
$[90,14,46]$	$40,41,14$	3	10	3	10	$37,47,6$	$(37,47)$	$[5,4,2]$	$[5,4,2]$
$[86,11,47]$	$1,43,11$	6	10	1	7	$0,50,6$	$(0,50)$	$[1,1,1]$	$[5,4,2]$
$[89,12,47]$	$40,41,14$	3	10	3	10	$37,47,6$	$(37,47)$	$[5,4,2]$	$[4,2,3]$
$[92,14,47]$	$40,41,14$	3	10	3	10	$37,47,6$	$(37,47)$	$[5,4,2]$	$[7,4,3]$
$[94,15,47]$	$41,40,15$	3	10	4	11	$37,47,6$	$(37,47)$	$[9,5,4]$	$[5,4,2]$
$[91,12,48]$	$40,41,14$	3	10	3	10	$37,47,6$	$(37,47)$	$[7,4,3]$	$[4,2,3]$
$[94,14,48]$	$40,41,14$	3	10	3	10	$37,47,6$	$(37,47)$	$[7,4,3]$	$[7,4,3]$
$[96,15,48]$	$41,40,15$	3	10	4	11	$37,47,6$	$(37,47)$	$[9,5,4]$	$[7,4,3]$
$[98,16,48]$	$41,39,16$	4	11	4	11	$37,47,6$	$(37,47)$	$[9,5,4]$	$[9,5,4]$
$[91,11,51]$	$1,43,11$	6	10	1	7	$0,50,6$	$(0,50)$	$[1,1,1]$	$[10,4,6]$
$[101,15,51]$	$1,40,15$	9	14	1	7	$0,50,6$	$(0,50)$	$[1,1,1]$	$[20,8,9]$
$[95,10,53]$	$37,44,10$	3	6	6	6	$31,53,2$	$(31,59)$	$[10,4,6]$	$[5,4,2]$
$[105,14,53]$	$40,41,14$	3	6	9	10	$31,53,2$	$(31,59)$	$[20,8,9]$	$[5,4,2]$
$[85,7,54]$	$1,49,7$	3	6	1	5	$0,53,4$	$(0,53)$	$[1,1,1]$	$[4,2,3]$
$[97,10,54]$	$37,44,10$	3	6	6	6	$31,53,2$	$(31,59)$	$[10,4,6]$	$[7,4,3]$
$[99,11,54]$	$1,43,11$	9	10	1	5	$0,53,4$	$(0,53)$	$[1,1,1]$	$[18,6,9]$
$[107,14,54]$	$40,41,14$	3	6	9	10	$31,53,2$	$(31,59)$	$[20,8,9]$	$[7,4,3]$
$[109,15,54]$	$1,40,15$	12	14	1	5	$0,53,4$	$(0,53)$	$[1,1,1]$	$[28,10,12]$
$[101,10,55]$	$37,44,10$	3	6	6	6	$31,53,2$	$(31,59)$	$[13,4,7]$	$[8,4,4]$
$[103,11,55]$	$37,43,11$	4	7	6	6	$31,53,2$	$(31,59)$	$[13,4,7]$	$[10,5,5]$
$[105,11,56]$	$37,43,11$	4	7	6	6	$31,53,2$	$(31,59)$	$[14,4,8]$	$[11,5,6]$
$[125,7,78]$	$1,49,7$	30	6	1	1	$0,80,0$	$(0,80)$	$[1,1,1]$	$[44,6,27]$

$w = 121$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[140,101,12]$	$55,6,101$	2	91	3	96	$52,11,86$	$(52,11)$	$[13,10,3]$	$[6,5,2]$
$[131,91,13]$	$53,10,91$	1	86	1	86	$52,12,81$	$(52,12)$	$[5,5,1]$	$[5,5,1]$
$[128,81,16]$	$1,12,81$	3	80	1	76	$0,16,75$	$(0,16)$	$[1,1,1]$	$[6,5,2]$
$[126,78,17]$	$1,12,81$	3	80	1	76	$0,16,75$	$(0,16)$	$[1,1,1]$	$[4,2,3]$
$[130,81,17]$	$1,12,81$	3	80	1	76	$0,16,75$	$(0,16)$	$[1,1,1]$	$[8,5,3]$
$[133,82,17]$	$1,10,86$	5	85	1	76	$0,16,75$	$(0,16)$	$[1,1,1]$	$[11,6,5]$
$[136,84,17]$	$1,10,86$	5	85	1	76	$0,16,75$	$(0,16)$	$[1,1,1]$	$[14,8,5]$
$[131,78,18]$	$49,12,81$	2	76	3	76	$46,17,71$	$(46,17)$	$[4,2,3]$	$[6,5,2]$
$[135,81,18]$	$49,12,81$	2	76	3	76	$46,17,71$	$(46,17)$	$[8,5,3]$	$[6,5,2]$
$[133,71,22]$	$44,17,71$	2	66	3	66	$41,22,61$	$(41,22)$	$[6,5,2]$	$[6,5,2]$
$[131,68,23]$	$44,17,71$	2	66	3	66	$41,22,61$	$(41,20)$	$[4,2,3]$	$[6,5,2]$
$[135,71,23]$	$44,17,71$	2	66	3	66	$41,22,61$	$(41,22)$	$[8,5,3]$	$[6,5,2]$
$[129,16,65]$	$61,60,16$	2	11	6	15	$55,68,10$	$(55,68)$	$[6,5,2]$	$[2,1,2]$
$[134,16,69]$	$61,60,16$	2	11	6	15	$55,68,10$	$(55,68)$	$[11,5,6]$	$[2,1,2]$
$[129,11,71]$	$55,66,11$	2	6	9	10	$46,77,5$	$(46,80)$	$[6,5,2]$	$[2,1,2]$
$[134,11,75]$	$55,66,11$	2	6	9	10	$46,77,5$	$(46,80)$	$[11,5,6]$	$[2,1,2]$

3.3.3 $q = 4$

$w = 51$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[53,6,36]$	$1,33,6$	1	5	1	5	$0,35,4$	$(0,35)$	$[1,1,1]$	$[1,1,1]$

$w = 63$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[69,50,9]$	$16,6,50$	1	47	1	47	$15,8,44$	$(15,8)$	$[3,3,1]$	$[3,3,1]$
$[73,53,9]$	$17,5,53$	1	47	2	50	$15,8,44$	$(15,8)$	$[7,6,2]$	$[3,3,1]$
$[68,48,10]$	$1,6,48$	2	47	1	45	$0,9,44$	$(0,9)$	$[1,1,1]$	$[4,3,2]$
$[71,50,10]$	$19,5,50$	2	47	2	47	$17,9,44$	$(17,9)$	$[4,3,2]$	$[4,3,2]$
$[67,45,11]$	$1,8,45$	1	44	1	42	$0,10,41$	$(0,10)$	$[1,1,1]$	$[3,3,1]$
$[70,47,11]$	$15,7,47$	1	44	2	44	$13,10,41$	$(13,10)$	$[4,3,2]$	$[3,3,1]$
$[75,50,11]$	$16,6,50$	1	44	3	47	$13,10,41$	$(13,10)$	$[9,6,3]$	$[3,3,1]$
$[69,44,12]$	$13,9,44$	1	41	1	41	$12,11,38$	$(12,11)$	$[3,3,1]$	$[3,3,1]$
$[69,41,13]$	$12,10,41$	1	38	1	38	$11,12,35$	$(11,12)$	$[3,3,1]$	$[3,3,1]$
$[73,44,13]$	$13,9,44$	1	38	2	41	$11,12,35$	$(11,12)$	$[7,6,2]$	$[3,3,1]$
$[68,39,14]$	$1,10,39$	2	38	1	36	$0,13,35$	$(0,13)$	$[1,1,1]$	$[4,3,2]$
$[71,41,14]$	$15,9,41$	2	38	2	38	$13,13,35$	$(13,13)$	$[4,3,2]$	$[4,3,2]$
$[73,42,14]$	$1,9,42$	3	41	1	36	$0,13,35$	$(0,13)$	$[1,1,1]$	$[9,6,3]$
$[67,36,15]$	$1,12,36$	1	35	1	33	$0,14,32$	$(0,14)$	$[1,1,1]$	$[3,3,1]$
$[70,38,15]$	$11,11,38$	1	35	2	35	$9,14,32$	$(9,14)$	$[4,3,2]$	$[3,3,1]$
$[76,33,21]$	$1,13,33$	7	32	1	27	$0,21,26$	$(0,21)$	$[1,1,1]$	$[12,6,6]$
$[73,30,22]$	$1,14,30$	6	29	1	27	$0,21,26$	$(0,21)$	$[1,1,1]$	$[9,3,6]$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[78,33,22]$	$1,13,33$	7	32	1	27	$0,21,26$	$(0,21)$	$[1,1,1]$	$[14,6,7]$
$[82,36,22]$	$1,12,36$	8	35	1	27	$0,21,26$	$(0,21)$	$[1,1,1]$	$[18,9,8]$
$[76,30,23]$	$7,14,30$	1	26	7	29	$0,22,25$	$(0,22)$	$[12,4,7]$	$[1,1,1]$
$[80,33,23]$	$8,13,33$	1	26	8	32	$0,22,25$	$(0,22)$	$[16,7,8]$	$[1,1,1]$
$[67,26,24]$	$1,21,26$	1	25	1	23	$0,23,22$	$(0,23)$	$[1,1,1]$	$[3,3,1]$
$[69,27,24]$	$1,20,27$	2	26	1	23	$0,23,22$	$(0,23)$	$[1,1,1]$	$[5,4,2]$
$[69,25,25]$	$21,22,25$	1	22	1	22	$20,24,19$	$(20,24)$	$[3,3,1]$	$[3,3,1]$
$[69,23,27]$	$1,22,23$	3	22	1	20	$0,26,29$	$(0,26)$	$[1,1,1]$	$[5,3,3]$
$[74,26,27]$	$1,21,26$	4	25	1	20	$0,26,19$	$(0,26)$	$[1,1,1]$	$[10,6,4]$
$[67,20,28]$	$1,25,20$	1	19	1	17	$0,27,16$	$(0,27)$	$[1,1,1]$	$[3,3,1]$
$[71,22,28]$	$20,23,22$	1	19	3	19	$17,27,16$	$(17,27)$	$[5,3,3]$	$[3,3,1]$
$[73,23,28]$	$20,22,23$	2	20	3	19	$17,27,16$	$(17,27)$	$[5,3,3]$	$[5,4,2]$
$[76,25,28]$	$21,22,25$	1	19	4	22	$17,27,16$	$(17,27)$	$[10,6,4]$	$[3,3,1]$
$[78,26,28]$	$21,21,26$	2	20	4	22	$17,27,16$	$(17,27)$	$[10,6,4]$	$[5,4,2]$
$[69,19,29]$	$17,26,19$	1	16	1	16	$16,28,13$	$(16,28)$	$[3,3,1]$	$[3,3,1]$
$[71,20,29]$	$1,25,20$	4	19	1	14	$0,30,13$	$(0,30)$	$[1,1,1]$	$[7,6,2]$
$[75,22,29]$	$21,23,22$	3	16	4	19	$17,30,13$	$(17,30)$	$[7,6,2]$	$[5,3,3]$
$[80,25,29]$	$21,22,25$	4	19	4	19	$17,30,13$	$(17,30)$	$[7,6,2]$	$[10,6,4]$
$[69,17,31]$	$1,26,17$	3	16	1	14	$0,30,13$	$(0,30)$	$[1,1,1]$	$[5,3,3]$
$[74,20,31]$	$1,25,20$	4	19	1	14	$0,30,13$	$(0,30)$	$[1,1,1]$	$[10,6,4]$
$[78,22,31]$	$21,23,22$	3	16	4	19	$17,30,13$	$(17,30)$	$[10,6,4]$	$[5,3,3]$
$[83,25,31]$	$21,22,25$	4	19	4	19	$17,30,13$	$(17,30)$	$[10,6,4]$	$[10,6,4]$
$[70,7,48]$	$1,42,7$	4	6	1	4	$0,47,3$	$(0,47)$	$[1,1,1]$	$[6,3,4]$
$[73,8,48]$	$1,41,8$	5	7	1	4	$0,47,3$	$(0,47)$	$[1,1,1]$	$[9,4,5]$

$w = 85$

$\mathcal{E}$	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[93,69,10]$	$29,5,69$	2	65	2	67	$27,9,63$	$(27,9)$	$[5,4,2]$	$[3,2,2]$
$[94,67,11]$	$29,7,67$	1	63	2	63	$27,10,59$	$(27,10)$	$[5,4,2]$	$[4,4,1]$

3.4 Konstruktion X^3

Sei $\mathcal{C}_1 \supseteq \mathcal{C}_2 \supseteq \mathcal{C}_3$ eine Kette linearer, q-ärer Codes mit den Parametern $[w,k_1,d_1]$, $[w,k_2,d_2]$ bzw. $[w,k_3,d_3]$. Sei desweiteren $\mathcal{C}' \subseteq \mathcal{C}_1$ ein $[w,k',d_1']$. Wenden wir Konstruktion X mit dem Hilfscode $\mathcal{D}_1 = [n_1, k_1 - k', \delta_1]$ auf $\mathcal{C}_1$ und $\mathcal{C}'$ an, so erhalten wir $\bar{\mathcal{C}}_1$ einen $[w+n_1, k_1, \mathrm{Min}(d_1', d_1+\delta_1)]$. Seien $\bar{\mathcal{C}}_2$ und $\bar{\mathcal{C}}_3$ die Bilder von $\mathcal{C}_2$ bzw. $\mathcal{C}_3$ in $\bar{\mathcal{C}}_1$. Man erhält $\bar{\mathcal{C}}_i$ aus Konstruktion X mit den Codes $\mathcal{C}_i$ und $\mathcal{C}_i \cap \mathcal{C}'$ mit einem geeigneten Teilcode von $\mathcal{D}_1$ als Hilfscode. Sei d_i' die Distanz von $\mathcal{C}_i \cap \mathcal{C}'$, so ist $\bar{\mathcal{C}}_i$ ein $[w+n_1, k_i, \mathrm{Min}(d_i', d_i+\delta_1)]$. Wenden wir nun die iterierte Konstruktion X auf $\bar{\mathcal{C}}_1 \supseteq \bar{\mathcal{C}}_2 \supseteq \bar{\mathcal{C}}_3$, mit Hilfscodes $\mathcal{D}_2 = [n_2, k_1 - k_2, \delta_2]$ und $\mathcal{D}_3 = [n_3, k_1 - k_3, \delta_3]$ an. So erhalten wir einen $[w+n_1+n_2+n_3, k, d]$ wobei $d = \mathrm{Min}(\mathrm{Min}(d_1', d_1+\delta_1)+\delta_2+\delta_3, \mathrm{Min}(d_2', d_2+\delta_1)+\delta_3, \mathrm{Min}(d_3', d_3+\delta_1))$ ist. Orientiert man sich an der Benennung der klassischen Konstruktionen, so sollte man diese Konstruktion X^3 nennen. Wir haben also:

Satz 3.5 (Konstruktion X^3) *Seien $\mathcal{C}_1 \supseteq \mathcal{C}_2 \supseteq \mathcal{C}_3$ lineare, q-äre Codes mit den Parametern $[w, k_1, d_1]$, $[w, k_2, d_2]$ bzw. $[w, k_3, d_3]$. Sei desweiteren $\mathcal{C}' \subseteq \mathcal{C}_1$ ein $[w, k', d'_1]$. Existieren Hilfscodes $\mathcal{D}_1 = [n_1, k_1 - k', \delta_1]$, $\mathcal{D}_2 = [n_2, k_1 - k_2, \delta_2]$ und $\mathcal{D}_3 = [n_3, k_1 - k_3, \delta_3]$. Sei d'_2 die Distanz von $\mathcal{C}_2 \cap \mathcal{C}'$, d'_3 die Distanz von $\mathcal{C}_3 \cap \mathcal{C}'$ und sei $d = \mathrm{Min}(\mathrm{Min}(d'_1, d_1 + \delta_1) + \delta_2 + \delta_3, \mathrm{Min}(d'_2, d_2 + \delta_1) + \delta_3, d'_3, d_3 + \delta_1)$. So gibt es einen*

$$[w + n_1 + n_2 + n_3, k, d].$$

Auch hier bringt eine Verallgemeinerung der Konstruktion auf längere Ketten von Codes keine neuen Ergebnisse in den von uns betrachteten Fällen. Der Fall der Ketten der Länge zwei ist Konstruktion XX. Bilden die $\mathcal{C}_i$ und $\mathcal{C}'$ eine Kette von vier Codes, so ist die Konstruktion äquivalent zur iterierten Konstruktion X auf einer Kette von vier Codes. Da wir etwas neues bekommen wollen, betrachten wir in den Anwendungen nur die Fälle bei denen $\mathcal{C}'$ und $\mathcal{C}_2$ oder $\mathcal{C}_3$ sich nicht trivial schneiden.

Wenden wir diesen Satz nun wieder auf BCH-Codes an. Eine (hinreichende) Bedingung, daß der Schnitt der BCH-Codes $\mathcal{B}(l, t)$ und $\mathcal{B}(l', t')$ wieder ein BCH-Code ist, ist, daß die Vereinigung der Intervalle $l, \ldots, t+l-1$ und $l', \ldots, t'+l'-1$ modulo w wieder ein Intervall bildet. Dies ist bei obiger Konstellation immer der Fall, da alle am Schnitt beteiligten Codes in $\mathcal{C}_1 = \mathcal{B}(l_1, t_1)$ liegen, also das Intervall $l_1, \ldots, t_1 + l_1 - 1$ enthalten. Ist l der Beginn des vereinigten Intervalls, so endet dieses,falls nicht $\mathcal{B}(l, t) \subset \mathcal{B}(l', t')$, mit $l' + t' - 1$. Die Distanz des Schnittes ist also mindestens $l' - l + t' + 1$. (Analog bekommt man als Distanz des Schnittes $l - l' + t + 1$, wenn l' der Beginn des vereinigten Intervalls ist.) Wie schon bei Konstruktion XX benutzen wir die Tatsache, daß der Schnitt zweier BCH-Codes eine größere designte Distanz als $l' - l + t' + 1$ haben kann. Ebenfalls wie in den vorigen Konstruktionen benutzen wir als $\mathcal{C}_1$ und $\mathcal{C}'$ bei Bedarf geeignete Teilcodes der BCH-Codes, so daß weiterhin $\mathcal{C}_1 \supset \mathcal{C}', \mathcal{C}_2$ gilt und die Schnitte von $\mathcal{C}'$ mit den Teilcodes dieselben bleiben. $\mathcal{C}_1$ hat also mindestens Dimension $\dim \mathcal{C}' + \dim \mathcal{C}_2 - \dim \mathcal{C}' \cap \mathcal{C}_2$. Setzen wir also $\mathcal{C}_1 \subset \mathcal{B}(l_1, t_1)$, $\mathcal{C}_2 = \mathcal{B}(l_2, t_2)$, $\mathcal{C}_3 = \mathcal{B}(l_3, t_3)$ und $\mathcal{C}' \subset \mathcal{B}(l'_1, t'_1)$, so bekommen wir folgende Konstruktion:

Satz 3.6 *Sei w ein Teiler von $q^r - 1$. Seien $t_1 > t_2 > t_3$ und $t_1 > t'_1$. Seien $l_1, l_2, l_3, l'_1 \in \mathbb{N}$, so daß bei Wahl von $0, \ldots, w-1$ als Vertretersystem modulo w gilt: $t_2 - t_1 \geq ((l_1 - l_2) \mod w)$, $t_3 - t_2 \geq ((l_2 - l_3) \mod w)$ und $t'_1 - t_1 \geq ((l_1 - l'_1) \mod w)$. Sei d'_i die maximale designte Distanz von $\mathcal{B}(l_i, t_i) \cap \mathcal{B}(l'_1, t'_1)$ für $i = 2, 3$. Seien $k_i := k(l_i, t_i)$ und $k'_i := dim(\mathcal{B}(l_i, t_i) \cap \mathcal{B}(l'_1, t'_1))$, für $i = 1, 2, 3$. Sei $k, k' \in \mathbb{N}$, so daß $k_1 \geq k > k' + k_2 - k'_2$. Existieren Hilfscodes $\mathcal{D}_1$, $\mathcal{D}_2$ und $\mathcal{D}_3$ mit den Parametern $[n_1, k - k', \delta_1]$, $[n_2, k - k(l_2, t_2), \delta_2]$ und $[n_3, k - k(l_3, t_3), \delta_3]$. So existiert ein linearer, q-ärer Code $\mathcal{E}$ mit den Parametern $[w + n_1 + n_2 + n_3, k, d]$ wobei $d = 1 + \mathrm{Min}(\mathrm{Min}(t'_1, t_1 + \delta_1) + \delta_2 + \delta_3, \mathrm{Min}(t'_2, t_2 + \delta_1) + \delta_3, t'_3, t_3 + \delta_1)$.*

Mit obigen Bezeichnungen erhalten wir nachfolgende neue Codes. Dabei erhält man k als Dimension von $\mathcal{E}$ und k' als $k - \dim \mathcal{D}_1$.

3.4.1 $q = 2$

$w = 127$

$\mathcal{E}$	l_1, t_1, k_1	l_2, t_2, k_2	l_3, t_3, k_3	l'_1, t'_1, k'_1	d'_2, k'_2	d'_3, k'_3	$\mathcal{D}_1$	$\mathcal{D}_2$	$\mathcal{D}_3$
$[152, 79, 22]$	$0, 13, 84$	$0, 15, 77$	$0, 19, 70$	$125, 15, 77$	$18, 70$	$22, 63$	$[8, 7, 2]$	$[3, 2, 2]$	$[14, 9, 4]$
$[154, 80, 22]$	$0, 13, 84$	$0, 15, 77$	$0, 19, 70$	$125, 15, 77$	$18, 70$	$22, 63$	$[8, 7, 2]$	$[4, 3, 2]$	$[15, 10, 4]$
$[160, 23, 57]$	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$123, 47, 21$	$52, 14$	$64, 7$	$[9, 8, 2]$	$[4, 1, 4]$	$[20, 8, 8]$
$[167, 26, 57]$	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$123, 47, 21$	$52, 14$	$64, 7$	$[9, 8, 2]$	$[8, 4, 4]$	$[23, 11, 8]$
$[164, 24, 58]$	$0, 43, 28$	$0, 47, 21$	$0, 55, 14$	$123, 47, 21$	$52, 14$	$64, 7$	$[8, 7, 2]$	$[7, 3, 4]$	$[22, 10, 8]$
$[166, 25, 58]$	$0, 43, 28$	$0, 47, 21$	$0, 55, 14$	$123, 47, 21$	$52, 14$	$64, 7$	$[8, 7, 2]$	$[8, 4, 4]$	$[23, 11, 8]$
$[164, 23, 59]$	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$123, 47, 21$	$52, 14$	$64, 7$	$[13, 8, 4]$	$[4, 1, 4]$	$[20, 8, 8]$
$[171, 26, 59]$	$1, 42, 29$	$1, 46, 22$	$1, 54, 15$	$123, 47, 21$	$52, 14$	$64, 7$	$[13, 8, 4]$	$[8, 4, 4]$	$[23, 11, 8]$
$[170, 25, 60]$	$0, 43, 28$	$0, 47, 21$	$0, 55, 14$	$123, 47, 21$	$52, 14$	$64, 7$	$[12, 7, 4]$	$[8, 4, 4]$	$[23, 11, 8]$

$w = 255$

$\mathcal{E}$	l_1, t_1, k_1	l_2, t_2, k_2	l_3, t_3, k_3	l'_1, t'_1, k'_1	d'_2, k'_2	d'_3, k'_3	$\mathcal{D}_1$	$\mathcal{D}_2$	$\mathcal{D}_3$
$[275, 231, 12]$	$1, 10, 215$	$0, 11, 214$	$253, 13, 206$	$1, 12, 207$	$14, 206$	$16, 198$	$[9, 8, 2]$	$[1, 1, 1]$	$[10, 9, 2]$
$[278, 216, 16]$	$0, 9, 222$	$0, 11, 214$	$0, 13, 206$	$253, 11, 214$	$14, 206$	$16, 198$	$[9, 8, 2]$	$[3, 2, 2]$	$[11, 10, 2]$
$[264, 192, 20]$	$1, 14, 199$	$1, 16, 191$	$1, 18, 187$	$0, 15, 198$	$18, 190$	$20, 186$	$[1, 1, 1]$	$[2, 1, 2]$	$[6, 5, 2]$
$[266, 193, 20]$	$1, 14, 199$	$1, 16, 191$	$1, 18, 187$	$0, 15, 198$	$18, 190$	$20, 186$	$[1, 1, 1]$	$[3, 2, 2]$	$[7, 6, 2]$
$[271, 191, 22]$	$1, 16, 191$	$0, 17, 190$	$253, 19, 182$	$1, 18, 187$	$20, 186$	$22, 178$	$[5, 4, 2]$	$[1, 1, 1]$	$[10, 9, 2]$
$[274, 192, 22]$	$0, 15, 198$	$0, 17, 190$	$0, 19, 186$	$253, 17, 190$	$20, 182$	$22, 178$	$[9, 8, 2]$	$[3, 2, 2]$	$[7, 6, 2]$
$[275, 187, 24]$	$1, 18, 187$	$0, 19, 186$	$253, 21, 178$	$1, 20, 179$	$22, 178$	$24, 170$	$[9, 8, 2]$	$[1, 1, 1]$	$[10, 9, 2]$
$[278, 188, 24]$	$0, 17, 190$	$0, 19, 186$	$0, 21, 178$	$253, 19, 182$	$22, 178$	$24, 170$	$[9, 8, 2]$	$[3, 2, 2]$	$[11, 10, 2]$
$[275, 179, 26]$	$1, 20, 179$	$0, 21, 178$	$253, 23, 170$	$1, 22, 171$	$24, 170$	$26, 162$	$[9, 8, 2]$	$[1, 1, 1]$	$[10, 9, 2]$
$[278, 180, 26]$	$0, 19, 186$	$0, 21, 178$	$0, 23, 170$	$253, 21, 178$	$24, 170$	$26, 162$	$[9, 8, 2]$	$[3, 2, 2]$	$[11, 10, 2]$
$[275, 171, 28]$	$1, 22, 171$	$0, 23, 170$	$253, 25, 162$	$1, 24, 163$	$26, 162$	$28, 154$	$[9, 8, 2]$	$[1, 1, 1]$	$[10, 9, 2]$
$[278, 172, 28]$	$0, 21, 178$	$0, 23, 170$	$0, 25, 162$	$253, 23, 170$	$26, 162$	$28, 154$	$[9, 8, 2]$	$[3, 2, 2]$	$[11, 10, 2]$
$[275, 163, 30]$	$1, 24, 163$	$0, 25, 162$	$253, 27, 154$	$1, 26, 155$	$28, 154$	$30, 146$	$[9, 8, 2]$	$[1, 1, 1]$	$[10, 9, 2]$
$[278, 164, 30]$	$0, 23, 170$	$0, 25, 162$	$0, 27, 154$	$253, 25, 162$	$28, 154$	$30, 146$	$[9, 8, 2]$	$[3, 2, 2]$	$[11, 10, 2]$
$[275, 155, 32]$	$1, 26, 155$	$0, 27, 154$	$253, 29, 146$	$1, 28, 147$	$30, 146$	$32, 138$	$[9, 8, 2]$	$[1, 1, 1]$	$[10, 9, 2]$
$[278, 156, 32]$	$0, 25, 162$	$0, 27, 154$	$0, 29, 146$	$253, 27, 154$	$30, 146$	$32, 138$	$[9, 8, 2]$	$[3, 2, 2]$	$[11, 10, 2]$
$[275, 115, 48]$	$1, 42, 115$	$0, 43, 114$	$253, 45, 106$	$1, 44, 107$	$46, 106$	$48, 98$	$[9, 8, 2]$	$[1, 1, 1]$	$[10, 9, 2]$
$[266, 92, 54]$	$1, 46, 99$	$1, 50, 91$	$1, 52, 87$	$0, 47, 98$	$52, 90$	$54, 86$	$[1, 1, 1]$	$[4, 1, 4]$	$[6, 5, 2]$
$[271, 91, 56]$	$1, 50, 91$	$0, 51, 90$	$253, 53, 82$	$1, 52, 87$	$54, 86$	$56, 78$	$[5, 4, 2]$	$[1, 1, 1]$	$[10, 9, 2]$

3.4.2 $q = 3$

$w = 26$

$\mathcal{E}$	l_1, t_1, k_1	l_2, t_2, k_2	l_3, t_3, k_3	l'_1, t'_1, k'_1	d'_2, k'_2	d'_3, k'_3	$\mathcal{D}_1$	$\mathcal{D}_2$	$\mathcal{D}_3$
$[33, 8, 17]$	$1, 12, 8$	$1, 13, 7$	$1, 16, 4$	$0, 13, 7$	$15, 6$	$18, 3$	$[1, 1, 1]$	$[1, 1, 1]$	$[5, 4, 2]$

$w = 80$

$\mathcal{E}$	l_1, t_1, k_1	l_2, t_2, k_2	l_3, t_3, k_3	l'_1, t'_1, k'_1	d'_2, k'_2	d'_3, k'_3	$\mathcal{D}_1$	$\mathcal{D}_2$	$\mathcal{D}_3$
$[86, 57, 12]$	$1, 7, 60$	$1, 9, 56$	$1, 10, 54$	$0, 8, 59$	$11, 55$	$12, 53$	$[1, 1, 1]$	$[2, 1, 2]$	$[3, 3, 1]$
$[92, 61, 12]$	$1, 6, 64$	$1, 7, 60$	$1, 10, 54$	$0, 7, 63$	$9, 59$	$12, 53$	$[1, 1, 1]$	$[1, 1, 1]$	$[10, 7, 3]$
$[88, 55, 14]$	$1, 9, 56$	$1, 10, 54$	$1, 12, 50$	$0, 10, 55$	$12, 53$	$14, 49$	$[1, 1, 1]$	$[1, 1, 1]$	$[6, 5, 2]$
$[93, 57, 14]$	$1, 7, 60$	$1, 9, 56$	$1, 12, 50$	$0, 8, 59$	$11, 55$	$14, 49$	$[1, 1, 1]$	$[2, 1, 2]$	$[10, 7, 3]$
$[98, 54, 17]$	$0, 10, 55$	$0, 11, 53$	$0, 13, 49$	$77, 13, 47$	$15, 45$	$17, 41$	$[11, 8, 3]$	$[1, 1, 1]$	$[6, 5, 2]$
$[88, 35, 23]$	$1, 16, 38$	$1, 19, 34$	$1, 21, 32$	$0, 17, 37$	$21, 33$	$23, 31$	$[1, 1, 1]$	$[3, 1, 3]$	$[4, 3, 2]$
$[102, 21, 39]$	$1, 24, 24$	$1, 25, 20$	$1, 39, 16$	$0, 25, 23$	$27, 19$	$41, 15$	$[1, 1, 1]$	$[1, 1, 1]$	$[20, 5, 12]$
$[88, 16, 44]$	$1, 39, 16$	$1, 40, 15$	$1, 43, 11$	$0, 40, 15$	$42, 14$	$45, 10$	$[1, 1, 1]$	$[1, 1, 1]$	$[6, 5, 2]$
$[92, 15, 46]$	$0, 40, 15$	$0, 41, 14$	$0, 44, 10$	$77, 43, 11$	$45, 10$	$48, 6$	$[5, 4, 2]$	$[1, 1, 1]$	$[6, 5, 2]$
$[96, 16, 47]$	$1, 39, 16$	$1, 40, 15$	$1, 43, 11$	$77, 43, 11$	$45, 10$	$48, 6$	$[9, 5, 4]$	$[1, 1, 1]$	$[6, 5, 2]$
$[95, 12, 51]$	$1, 40, 15$	$1, 43, 11$	$1, 49, 7$	$0, 41, 14$	$45, 10$	$51, 6$	$[1, 1, 1]$	$[3, 1, 3]$	$[11, 5, 6]$
$[97, 13, 51]$	$1, 40, 15$	$1, 43, 11$	$1, 49, 7$	$0, 41, 14$	$45, 10$	$51, 6$	$[1, 1, 1]$	$[4, 2, 3]$	$[12, 6, 6]$
$[103, 16, 51]$	$1, 39, 16$	$1, 40, 15$	$1, 49, 7$	$0, 40, 15$	$42, 14$	$51, 6$	$[1, 1, 1]$	$[1, 1, 1]$	$[21, 9, 9]$
$[102, 13, 52]$	$1, 40, 15$	$1, 43, 11$	$1, 49, 7$	$77, 44, 10$	$48, 6$	$60, 2$	$[6, 5, 2]$	$[4, 2, 3]$	$[12, 6, 6]$
$[108, 16, 52]$	$1, 39, 16$	$1, 40, 15$	$1, 49, 7$	$77, 43, 11$	$45, 10$	$60, 2$	$[6, 5, 2]$	$[1, 1, 1]$	$[21, 9, 9]$
$[97, 11, 53]$	$1, 43, 11$	$0, 44, 10$	$77, 47, 6$	$1, 49, 7$	$51, 6$	$60, 2$	$[10, 4, 6]$	$[1, 1, 1]$	$[6, 5, 2]$
$[101, 12, 53]$	$0, 41, 14$	$0, 44, 10$	$0, 50, 6$	$77, 44, 10$	$48, 6$	$60, 2$	$[5, 4, 2]$	$[4, 2, 3]$	$[12, 6, 6]$
$[107, 15, 53]$	$0, 40, 15$	$0, 41, 14$	$0, 50, 6$	$77, 43, 11$	$45, 10$	$60, 2$	$[5, 4, 2]$	$[1, 1, 1]$	$[21, 9, 9]$
$[103, 12, 54]$	$0, 41, 14$	$0, 44, 10$	$0, 50, 6$	$77, 44, 10$	$48, 6$	$60, 2$	$[7, 4, 3]$	$[4, 2, 3]$	$[12, 6, 6]$
$[105, 13, 54]$	$1, 40, 15$	$1, 43, 11$	$1, 52, 5$	$0, 41, 14$	$45, 10$	$54, 4$	$[1, 1, 1]$	$[4, 2, 3]$	$[20, 8, 9]$
$[111, 16, 54]$	$1, 39, 16$	$1, 40, 15$	$1, 52, 5$	$0, 40, 15$	$42, 14$	$54, 4$	$[1, 1, 1]$	$[1, 1, 1]$	$[29, 11, 12]$
$[96, 7, 60]$	$1, 49, 7$	$0, 50, 6$	$71, 59, 2$	$1, 52, 5$	$54, 4$	$81, 0$	$[4, 2, 3]$	$[1, 1, 1]$	$[11, 5, 6]$
$[129, 7, 81]$	$31, 49, 7$	$28, 52, 5$	$1, 79, 1$	$31, 50, 6$	$54, 4$	$81, 0$	$[1, 1, 1]$	$[4, 2, 3]$	$[44, 6, 27]$

3.4.3 $q = 4$

$w = 63$

$\mathcal{E}$	l_1, t_1, k_1	l_2, t_2, k_2	l_3, t_3, k_3	l'_1, t'_1, k'_1	d'_2, k'_2	d'_3, k'_3	$\mathcal{D}_1$	$\mathcal{D}_2$	$\mathcal{D}_3$
$[75, 31, 22]$	$1, 13, 33$	$1, 14, 30$	$1, 20, 27$	$0, 14, 32$	$16, 29$	$22, 26$	$[1, 1, 1]$	$[1, 1, 1]$	$[10, 4, 6]$
$[70, 24, 26]$	$1, 21, 26$	$1, 22, 23$	$1, 25, 20$	$0, 22, 25$	$24, 22$	$27, 19$	$[1, 1, 1]$	$[1, 1, 1]$	$[5, 4, 2]$
$[76, 27, 27]$	$1, 20, 27$	$1, 21, 26$	$1, 25, 20$	$0, 21, 26$	$23, 25$	$27, 19$	$[1, 1, 1]$	$[1, 1, 1]$	$[11, 7, 4]$
$[80, 27, 28]$	$1, 20, 27$	$1, 21, 26$	$1, 25, 20$	$62, 22, 23$	$24, 22$	$28, 16$	$[5, 4, 2]$	$[1, 1, 1]$	$[11, 7, 4]$
$[77, 23, 29]$	$1, 22, 23$	$0, 23, 22$	$59, 27, 16$	$1, 25, 20$	$27, 19$	$31, 13$	$[5, 3, 3]$	$[1, 1, 1]$	$[8, 7, 2]$
$[82, 26, 29]$	$0, 21, 26$	$0, 22, 25$	$0, 26, 19$	$59, 25, 20$	$27, 19$	$31, 13$	$[7, 6, 2]$	$[1, 1, 1]$	$[11, 7, 4]$
$[70, 18, 30]$	$1, 25, 20$	$1, 26, 17$	$1, 29, 14$	$0, 26, 19$	$28, 16$	$31, 13$	$[1, 1, 1]$	$[1, 1, 1]$	$[5, 4, 2]$
$[80, 23, 31]$	$1, 22, 23$	$0, 23, 22$	$59, 27, 16$	$1, 25, 20$	$27, 19$	$31, 13$	$[5, 3, 3]$	$[1, 1, 1]$	$[11, 7, 4]$
$[70, 8, 46]$	$1, 41, 8$	$1, 42, 7$	$1, 46, 4$	$0, 42, 7$	$44, 6$	$48, 3$	$[1, 1, 1]$	$[1, 1, 1]$	$[5, 4, 2]$
$[75, 7, 50]$	$0, 42, 7$	$0, 43, 6$	$0, 47, 3$	$59, 46, 4$	$48, 3$	$64, 0$	$[6, 3, 4]$	$[1, 1, 1]$	$[5, 4, 2]$
$[97, 8, 63]$	$1, 41, 8$	$0, 42, 7$	$43, 62, 1$	$1, 42, 7$	$44, 6$	$64, 0$	$[1, 1, 1]$	$[1, 1, 1]$	$[32, 7, 19]$

3.5 BCH-Codes größerer Distanz

Die Minimaldistanz eines BCH-Codes kann größer als seine designte Distanz sein. Ein solcher Fall, in dem uns interessierenden Bereich, ist der binäre primitive BCH-Code der Länge 127 und der designten Distanz 29, also der $\mathcal{B}(127, 1, 28)$; dieser hat Dimension 43. In [21] wurde gezeigt, daß die Minimaldistanz dieses Codes 31 ist, also daß $\mathcal{B}(127, 1, 28)$ sogar ein $[127, 43, 31]$ ist. Außerdem hat $\mathcal{B}(255, 1, 58)$ Distanz 61 und $\mathcal{B}(255, 1, 60)$ Distanz 63; dies sind also Codes $[255, 71, 61]$ bzw. $[255, 63, 63]$ [2]. Verwenden wir diese Distanzen in Konstruktion X, so bekommen wir folgende neue binäre Codes:

$\mathcal{E}$	$\bar{\mathcal{C}}$	(l, t)	$\mathcal{C}'$	(l', t')	$\mathcal{D}$
$[131, 44, 31]$	$[127, 50, 27]$	$(1, 26)$	$[127, 43, 31]$	$(1, 28)$	$[4, 1, 4]$
$[135, 47, 31]$	$[127, 50, 27]$	$(1, 26)$	$[127, 43, 31]$	$(1, 28)$	$[8, 4, 4]$
$[139, 50, 31]$	$[127, 50, 27]$	$(1, 26)$	$[127, 43, 31]$	$(1, 28)$	$[12, 7, 4]$
$[151, 55, 31]$	$[127, 57, 23]$	$(1, 22)$	$[127, 43, 31]$	$(1, 28)$	$[24, 12, 8]$
$[142, 43, 33]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[15, 14, 2]$
$[143, 40, 35]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[16, 11, 4]$
$[147, 43, 35]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[20, 14, 4]$
$[145, 38, 37]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[18, 9, 6]$
$[151, 43, 37]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[24, 14, 6]$
$[151, 41, 39]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[24, 12, 8]$
$[155, 43, 39]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[28, 14, 8]$
$[155, 39, 41]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[28, 10, 10]$
$[159, 42, 41]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[32, 13, 10]$
$[161, 43, 41]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[34, 14, 10]$
$[159, 40, 43]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[32, 11, 12]$
$[161, 41, 43]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[34, 12, 12]$
$[164, 43, 43]$	$[127, 43, 31]$	$(1, 28)$	$[127, 29, 43]$	$(1, 42)$	$[37, 14, 12]$
$[261, 72, 61]$	$[255, 79, 55]$	$(1, 54)$	$[255, 71, 61]$	$(1, 58)$	$[6, 1, 6]$
$[264, 73, 61]$	$[255, 79, 55]$	$(1, 54)$	$[255, 71, 61]$	$(1, 58)$	$[9, 2, 6]$
$[267, 75, 61]$	$[255, 79, 55]$	$(1, 54)$	$[255, 71, 61]$	$(1, 58)$	$[12, 4, 6]$
$[264, 71, 63]$	$[255, 71, 61]$	$(1, 58)$	$[255, 63, 63]$	$(1, 60)$	$[9, 8, 2]$

Verwenden wir die iterierte Konstruktion X und beachten auch hier, daß der $\mathcal{B}(127, 28, 1)$ (hier der innere Code) Distanz 31 hat, so erhalten wir folgende neue Codes:

$\mathcal{E}$	w	$l, t, k(l, t)$	$l', t', k(l', t')$	$l'', t'', k(l'', t'')$	$\mathcal{D}$	$\mathcal{D}'$
$[144, 51, 31]$	127	$1, 22, 57$	$1, 26, 50$	$1, 28, 43$	$[4, 1, 4]$	$[13, 8, 4]$
$[147, 52, 31]$	127	$1, 22, 57$	$1, 26, 50$	$1, 28, 43$	$[6, 2, 4]$	$[14, 9, 4]$

3.6 Konstruktion X4

Der all-1 Code, also den Code der aus dem Codewort das n mal den Eintrag 1 hat und dessen Vielfachen besteht, hat als dualen Code den linearen q-ären $[n, n-1, 2]$. Damit besteht der $[n, n-1, 2]$ aus allen Elementen in $\mathbb{F}_q^n$ die die Quersumme Null haben. Dies werden wir im folgenden benutzen, um ein Wort von maximalem Gewicht, oder äquivalent einen eindimensionalen Teilraum maximaler Distanz im $[n, n-1, 2]$ zu finden.

Für $q = 2$ haben wir: $\mathcal{B}(255, 1, 6) = [255, 231, 7] \supset \mathcal{B}(255, 1, 8) = [255, 223, 9]$. Außerdem haben wir uns oben überlegt, daß $[10, 9, 2] \supset [10, 1, 10]$. Konstruktion X4 (Bemerkung 1.16) liefert uns aus diesen Codes einen linearen, binären

$$[265, 232, 9].$$

Ebenso erhalten wir im Fall $q = 3$ aus den Codes $\mathcal{B}(82, 38, 7) = [82, 65, 8] \supset \mathcal{B}(82, 37, 9) = [82, 57, 10]$ und $[10, 9, 2] \supset [10, 1, 10]$ einen linearen, ternären

$$[92, 66, 10].$$

Die Konstruktionen XX und X^3 setzen sich aus mehreren Anwendungen von Konstruktion X zusammen, es liegt nahe, eine oder mehrere der Anwendungen von Konstruktion X durch Anwendung von Konstruktion X4 zu ersetzen.

Sei $q = 2$ und $w = 255$. Wir haben: $\mathcal{B}(1, 4) = [255, 239, 5] \supset \mathcal{B}(0, 5) = [255, 238, 6]$, $\mathcal{B}(1, 6) = [255, 231, 7]$ und $\mathcal{B}(0, 5) \cap \mathcal{B}(1, 6) = \mathcal{B}(0, 7) = [255, 230, 8]$. Wenden wir Konstruktion X auf $\mathcal{B}(1, 4) \supset \mathcal{B}(0, 5)$ mit Hilfscode $[1, 1, 1]$ an, so erhalten wir einen $[256, 239, 6]$, der einen $[256, 231, 8]$ enthält. Wenden wir auf dieses Paar Konstruktion X4 mit den Codes $[10, 9, 2] \supset [10, 1, 10]$ an, so erhalten wir einen linearen, binären

$$[266, 240, 8].$$

Es ist $\mathcal{B}(0, 1) = [255, 254, 2] \supset \mathcal{B}(251, 5) = [255, 238, 6], \mathcal{B}(0, 3) = [255, 246, 4]$ und $\mathcal{B}(251, 5) \cap \mathcal{B}(0, 3) = \mathcal{B}(251, 7) = [255, 230, 8]$. Wenden wir Konstruktion X auf $\mathcal{B}(0, 1) \supset \mathcal{B}(251, 5)$ mit Hilfscode $[22, 16, 4]$ an, so erhalten wir einen $[277, 254, 6]$, der einen $[277, 246, 8]$ enthält. Wenden wir auf dieses Paar Konstruktion X4 mit den Codes $[10, 9, 2] \supset [10, 1, 10]$ an, so erhalten wir einen linearen, binären

$$[287, 255, 8].$$

Es ist $\mathcal{B}(253, 3) = [255, 246, 4] \supset \mathcal{B}(251, 5) = [255, 238, 6], \mathcal{B}(253, 5) = [255, 238, 6]$ und $\mathcal{B}(251, 5) \cap \mathcal{B}(0, 3) = \mathcal{B}(251, 7) = [255, 230, 8]$. Wenden wir auf $\mathcal{B}(253, 3) \supset \mathcal{B}(251, 5)$ Konstruktion X4 mit den Codes $[10, 9, 2] \supset [10, 1, 10]$ an, so erhalten wir einen $[265, 247, 6]$, der einen $[265, 239, 8]$ enthält. Wenden wir auf dieses Paar wiederum Konstruktion X4 mit den Codes $[10, 9, 2] \supset [10, 1, 10]$ an, so erhalten wir einen linearen, binären

$$[275, 248, 8].$$

Es ist $\mathcal{B}(1,2) = [255, 247, 3] \supset \mathcal{B}(0,3) = [255, 246, 4] \supset \mathcal{B}(253,5) = [255, 238, 6]$, $\mathcal{B}(1,2) \supset \mathcal{B}(1,4) = [255, 239, 5]$ und $\mathcal{B}(1,4) \cap \mathcal{B}(0,3) = \mathcal{B}(0,5) = [255, 238, 6]$ und $\mathcal{B}(1,4) \cap \mathcal{B}(253,5) = \mathcal{B}(253,7) = [255, 230, 8]$. Wenden wir Konstruktion X4 auf $\mathcal{B}(1,2) \supset \mathcal{B}(1,4)$ mit $[10, 9, 2] \supset [10, 1, 10]$ an, so erhalten wir einen $[265, 248, 5]$, dieser enthält die Teilcodes $[265, 247, 6] \supset [265, 239, 8]$. Wenden wir auf $[265, 248, 5] \supset [265, 247, 6]$ Konstruktion X mit dem $[1, 1, 1]$ an, so erhalten wir einen $[266, 248, 6]$ mit Teilcode $[266, 239, 8]$. Wenden wir auf diese, Konstruktion X4 mit den Codes $[11, 10, 2] \supset [11, 1, 10]$ an, so erhalten wir einen

$$[277, 249, 8].$$

Es ist $\mathcal{B}(0,1) = [255, 254, 2] \supset \mathcal{B}(0,3) = [255, 246, 4] \supset \mathcal{B}(0,5) = [255, 238, 6]$, $\mathcal{B}(0,1) \supset \mathcal{B}(253,3) = [255, 246, 4]$, $\mathcal{B}(253,3) \cap \mathcal{B}(0,3) = \mathcal{B}(253,5) = [255, 238, 6]$ und $\mathcal{B}(253,3) \cap \mathcal{B}(0,5) = \mathcal{B}(253,7) = [255, 230, 8]$. Wenden wir Konstruktion X4 auf $\mathcal{B}(0,1) \supset \mathcal{B}(253,3)$ mit $[10, 9, 2] \supset [10, 1, 10]$ an, so erhalten wir einen $[265, 255, 4]$, dieser enthält die Teilcodes $[265, 247, 6] \supset [265, 239, 8]$. Wir benutzen von dem $[265, 255, 4]$ nur einen geeigneten Teilcode der Dimension 249. Wenden wir auf $[265, 249, 4] \supset [265, 247, 6]$ Konstruktion X mit dem $[3, 2, 2]$ an, so erhalten wir einen $[268, 249, 6]$ mit Teilcode $[268, 239, 8]$. Wenden wir auf diese Konstruktion X4 mit den Codes $[12, 11, 2] \supset [12, 1, 12]$ an, so erhalten wir einen

$$[280, 250, 8].$$

Benutzen wir von dem $[265, 255, 4]$ nur einen geeigneten Teilcode der Dimension $249+i$, so muß man auch bei jeden Hilfscode einen um i längeren Code verwenden und wir bekommen für $1 \leq i \leq 6$ einen

$$[280 + 3i, 250 + i, 8].$$

Es ist $\mathcal{B}(0,5) = [255, 238, 6] \supset \mathcal{B}(0,7) = [255, 230, 8] \supset \mathcal{B}(0,9) = [255, 222, 10]$, $\mathcal{B}(0,5) \supset \mathcal{B}(253,7) = [255, 230, 8]$, $\mathcal{B}(253,7) \cap \mathcal{B}(0,7) = \mathcal{B}(253,9) = [255, 222, 10]$ und $\mathcal{B}(253,7) \cap \mathcal{B}(0,9) = \mathcal{B}(253,11) = [255, 214, 8]$. Wenden wir Konstruktion X auf $\mathcal{B}(0,5) \supset \mathcal{B}(0,7)$ mit $[9, 8, 2]$ an, so erhalten wir einen $[264, 238, 8]$, dieser enthält die Teilcodes $[264, 230, 10] \supset [265, 222, 12]$. Wir benutzen von dem $[264, 238, 8]$ nur einen geeigneten Teilcode der Dimension 232. Wenden wir auf $[264, 232, 8] \supset [264, 230, 10]$ Konstruktion X mit dem $[3, 2, 2]$ an, so erhalten wir einen $[267, 232, 10]$ mit Teilcode $[267, 222, 12]$. Wenden wir auf diese Konstruktion X4 mit den Codes $[12, 11, 2] \supset [12, 1, 12]$ an, so erhalten wir einen

$$[279, 233, 12].$$

Die Checkmatrix des ternären Hammingcodes $[13, 10, 3]$ ist:

$$\begin{array}{c} 1111111110000 \\ 0120011221110 \\ 0001212120121 \end{array}$$

Das Wort 1111111111110 liegt also im Hammingcode, dieser besitzt damit einen $[13, 1, 12]$ als Teilcode. Nimmt man die Worte des Hammingcodes, die in der letzten Spalte eine Null stehen haben, so erhält man einen $[12, 9, 3]$ mit einem $[12, 1, 12]$ als Teilcode.

Sei $q = 3$ und $w = 80$. Es ist $\mathcal{B}(1, 6) = [80, 64, 7] \supset \mathcal{B}(0, 7) = [80, 63, 8], \mathcal{B}(1, 9) = [80, 56, 10]$ und $\mathcal{B}(0, 7) \cap \mathcal{B}(1, 9) = \mathcal{B}(0, 10) = [80, 55, 11]$. Wenden wir Konstruktion X auf $\mathcal{B}(1, 6) \supset \mathcal{B}(0, 7)$ mit Hilfscode $[1, 1, 1]$ an, so erhalten wir einen $[81, 64, 7]$, der einen $[81, 56, 11]$ enthält. Wenden wir auf dieses Paar Konstruktion X4 mit den Codes $[12, 9, 3] \supset [12, 1, 12]$ an, so erhalten wir einen linearen, ternären

$$[93, 65, 11].$$

Es ist $\mathcal{B}(37, 5) = [80, 67, 6] \supset \mathcal{B}(34, 8) = [80, 59, 9], \mathcal{B}(37, 7) = [80, 63, 8]$ und $\mathcal{B}(34, 8) \cap \mathcal{B}(37, 7) = \mathcal{B}(34, 10) = [80, 55, 11]$. Wenden wir Konstruktion X auf $\mathcal{B}(37, 5) \supset \mathcal{B}(37, 7)$ mit Hilfscode $[5, 4, 2]$ an, so erhalten wir einen $[85, 67, 8]$, der einen $[85, 59, 11]$ enthält. Wenden wir auf dieses Paar Konstruktion X4 mit den Codes $[12, 9, 3] \supset [12, 1, 12]$ an, so erhalten wir einen linearen, ternären

$$[97, 68, 11].$$

3.7 Einige duale Codes

Ist die Dimension bzw. die Codimension eines Codes klein genug, so kann man mit dem Computer alle Codeworte des Codes bzw. des dualen Codes erzeugen und deren Gewicht berechnen. Aus der so erhaltenen Gewichtsverteilung bekommt man so mittels MacWilliams-Transformation (Satz 2.4) die Gewichtsverteilung des dualen Codes bzw. des Codes und erhält so insbesondere dessen Minimaldistanz.

3.7.1 $q = 3$

Konstruktion XX mit $\tilde{\mathcal{C}} = \mathcal{B}(80, 1, 39) = [80, 16, 40] \supset \tilde{\mathcal{C}}_1 = \mathcal{B}(80, 1, 40) = [80, 15, 41], \tilde{\mathcal{C}}_2 = \mathcal{B}(80, 0, 40) = [80, 15, 41]$ und $\mathcal{C}' = \mathcal{B}(80, 0, 41) = [80, 14, 42]$ und den Hilfscodes $[1, 1, 1]$ und $[1, 1, 1]$ liefert einen $[82, 16, 42]$, dessen dualer Code ist ein

$$[82, 66, 8].$$

Der $[82, 16, 42]$ hat somit duale Distanz 8. Konstruktion Y1 (Bemerkung 1.20) liefert daraus einen

$$[74, 9, 42].$$

Die erweiterten BCH-Codes (siehe Bemerkung 2.28) $\hat{\mathcal{B}}(80, 1, 39) = [81, 16, 41]$, $\hat{\mathcal{B}}(80, 1, 40) = [81, 15, 42]$ und $\hat{\mathcal{B}}(80, 1, 43) = [81, 11, 45]$ haben duale Distanz 8,7 bzw. 6. Konstruktion X angewandt auf die dualen Codes $[81, 66, 7] \subset [81, 70, 6]$ mit Hilfscode $[4, 4, 1]$ liefert daraus einen

$$[85, 70, 7].$$

Konstruktion X angewandt auf die dualen Codes $[81, 65, 8] \subset [81, 70, 6]$ mit Hilfscode $[6, 5, 2]$ liefert daraus einen

$$[87, 70, 8].$$

Der duale des erweiterten Codes $\hat{\mathcal{B}}(80, 1, 3) = [81, 72, 5]$ ist ein

$$[81, 9, 48].$$

3.7.2 $q = 4$

Der erweiterte Code $\hat{\mathcal{B}}(63, 1, 4) = [64, 54, 6]$ hat duale Distanz 32. Konstruktion Y1 liefert daraus einen

$$[32, 23, 6].$$

Die erweiterten BCH-Codes $\hat{\mathcal{B}}(63, 1, 41) = [64, 8, 43]$ und $\hat{\mathcal{B}}(63, 1, 42) = [64, 7, 44]$ haben duale Distanz 5 bzw. 4. Damit haben wir folgende Kette dualer Codes: $[64, 56, 5] \subset [64, 57, 4]$. Konstruktion X mit Hilfscode $[1, 1, 1]$ liefert daraus einen

$$[65, 57, 5].$$

4 Codes für u=2

Sei w ein Teiler von $q^r - 1$ und $\phi : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ eine $\mathbb{F}_q$-lineare Abbildung mit u-dimensionalem Bild. In diesem Abschnitt wollen wir als Beispiel für die Codes $\phi(\mathcal{A}(w,l,t))^{\perp\!\!\!\perp}$, mit $u > 1$, den Fall $u = q = 2$ betrachten. Man erhält also quaternäre additive Codes. Abgesehen davon, daß dies der kleinste Fall ist und wir hier die ρ's besonderes einfach bestimmen können, bietet er sich an, da wir mit den linearen, quaternären Codes einen Vergleich für die Qualität der Codes bekommen.

Zu beachten ist, daß wenn die Dimension des Bildes von ϕ größer als eins ist, der Code nicht mehr unabhängig von der Wahl von ϕ ist. Zur Vereinfachung definieren wir folgende Notation:

Definition 4.1 *Ist ϕ gegeben, so definiere $\mathcal{C}(\phi,w,l,t) = \mathcal{C}(w,l,t) = \mathcal{C}(l,t) := \phi(\mathcal{A}(w,l,t))^{\perp\!\!\!\perp}$, wobei wir ϕ bzw. w weglassen, wenn diese aus dem Zusammenhang hervorgehen. Die $\mathbb{F}_q$-Dimension von $\mathcal{C}(\phi,w,l,t)$ sei $k(\phi,w,l,t) = k(w,l,t) = k(l,t)$. Damit hat $\mathcal{C}(w,l,t)$ die Parameter $[w,k(l,t),t+1]$.*

Nach Lemma 2.11 ist $k(\phi,w,l,t)$, die $\mathbb{F}_q$-Dimension des Codes, gerade:

$$k(\phi,w,l,t) = uw - rt + \rho(\phi,w,l,t)$$

Sei nun $u = 2$. Damit lassen sich die ρ's einfach rekursiv aus Satz 2.31 bestimmen. Von ϕ ist nur dessen Kern für die Bestimmung der ρ's von Bedeutung. Ist $\mathbf{U} :=$ Kern(ϕ) und α, β eine Basis von U^{tr}. Wegen Satz 2.12 können wir ObdA $\beta = 1$ setzen. Aus Satz 2.31 sehen wir, daß man für jeden Teilkörper, ungleich $\mathbb{F}_q$, von $\mathbb{F}_{q^r}$ eine Klasse von Codes mit verschiedenen Parametern bekommen, indem wir α als ein primitives Element des Teilkörpers wählen.

4.1 Additive quaternäre Codes

Sei nun also $u = q = 2$. Damit sind die Codes $\mathcal{C}(\phi,w,l,t)$ linear über $\mathbb{F}_2$ und quaternär. $\mathbb{F}_2$-Linearität ist dasselbe wie Additivität. Man beachte, daß ein $\mathbb{F}_2$-linearer, quaternärer Code $[n,k,d]$ nach Definition 2^k Codeworte hat. Betrachtet man also einen linearen, quaternären Code $[n,k,d]$, so hat dieser als $\mathbb{F}_2$-linearer, quaternärer Code die Parameter $[n,2k,d]$. Hier wollen wir die Codes $\mathcal{C}(\phi,w,l,t)$ mit linearen, quaternären Codes vergleichen.

Wie wir oben gesehen haben sind die Codeparameter für $r = 3,5,7$, also $w = 7,31$ bzw. 127, unabhängig von der Wahl von ϕ. Im Fall $r = 4$ bzw $r = 8$ stellt sich heraus, daß wir nur im linearen Fall neue Codes bekommen. Im Fall $r = 6$ haben wir drei verschiedene Klassen von Abbildungen ϕ. Die erste, der lineare Fall, wird

durch $\alpha = \zeta^{21}$ repräsentiert. Die zweite Klasse wird durch $\alpha = \zeta$ repräsentiert, diese Codes liefern nie bessere Parameter als die linearen (vergleiche das Beispiel in Abschnitt 2.3.3). Die dritte Klasse wird durch $\alpha = \zeta^9$ repräsentiert, dies ist der interessante Fall, dieser liefert für einige Distanzen bessere Parameter als der lineare Fall. Für alle folgenden Codes mit $w = 21$ oder $w = 63$ werden wir dieses ϕ benutzen, außer wir bemerken ausdrücklich, daß wir den linearen Fall verwenden. Ähnlich ist die Situation für $r = 10$, $w = 93$. Auch hier liefert der Fall $\alpha = \zeta^{33}$ für einige Distanzen bessere Parameter als der lineare Fall. Diesen Fall werden wir für alle folgenden Codes mit $w = 93$ verwenden.

Die folgenden Codes $\mathcal{C}(w, l, t)$ bzw. $\hat{\mathcal{C}}(w, t, 1)$ (die erweiterten Codes nach Bemerkung 2.28) haben mehr Codeworte, als der beste mir bekannte lineare, quaternäre Code gleicher Distanz und Länge.

$$\hat{\mathcal{C}}(7,1,1) = [8,11,3], \quad \hat{\mathcal{C}}(7,1,4) = [8,5,6],$$
$$\hat{\mathcal{C}}(31,1,4) = [32,47,6], \quad \hat{\mathcal{C}}(31,1,12) = [32,22,14], \quad \hat{\mathcal{C}}(31,1,22) = [32,7,24],$$
$$\mathcal{C}(21,7,17) = [21,3,18], \quad \mathcal{C}(63,19,53) = [63,3,54], \quad \mathcal{C}(63,55,17) = [63,58,18],$$
$$\hat{\mathcal{C}}(63,1,12) = [64,75,14], \quad \hat{\mathcal{C}}(63,1,17) = [64,57,19], \quad \hat{\mathcal{C}}(63,1,44) = [64,11,46],$$
$$\hat{\mathcal{C}}(127,1,4) = [128,233,6], \quad \hat{\mathcal{C}}(127,1,8) = [128,212,10],$$
$$\hat{\mathcal{C}}(127,1,12) = [128,191,14], \quad \hat{\mathcal{C}}(127,1,16) = [128,170,18],$$
$$\hat{\mathcal{C}}(127,1,18) = [128,163,20], \quad \hat{\mathcal{C}}(127,1,20) = [128,156,22],$$
$$\hat{\mathcal{C}}(127,1,24) = [128,135,26], \quad \hat{\mathcal{C}}(127,1,36) = [128,93,38],$$
$$\hat{\mathcal{C}}(127,1,44) = [128,72,46], \quad \hat{\mathcal{C}}(127,1,94) = [128,9,96],$$
$$\mathcal{C}(93,25,71) = [93,5,72].$$

Dabei haben die sieben ersten, bis auf den $[32, 22, 14]$, der $[64, 11, 46]$ und die beiden letzten Codes mehr Codewörter als ein linearer Code gleicher Distanz und Länge, nach den oberen Schranken in [8], überhaupt besitzen kann.

Desweiteren bekommt man mit den diversen Konstruktionen weitere $\mathbb{F}_2$-lineare, quaternäre Codes, die mehr Codeworte als der vergleichbare lineare Code haben. Hierbei sind die benutzten Hilfscodes entweder aus einem $\mathcal{C}(w, l, t)$, oder einem schon konstruierten $\mathbb{F}_2$-linearen, quaternären Code, mittels Bemerkung 1.12 abgeleitet. Dabei beachte man, daß ein linearer, quaternärer Code $[n, k, d]$ nach Bemerkung 2.2 auch ein $\mathbb{F}_2$-linearer, quaternärer Code $[n, 2k, d]$ ist. Man überzeugt sich sofort, daß man in den Sätzen 3.2, 3.4 und 3.6, sowie deren Herleitungen, $\mathcal{B}(w, l, t)$ durch $\mathcal{C}(w, l, t)$, ohne weitere Änderungen, ersetzen kann. Man erhält mit den Bezeichnungen aus diesen Sätzen folgende Codes:

4.1.1 Codes aus Konstruktion X

$\mathcal{E}$	$\bar{\mathcal{C}}$	(l,t)	$\mathcal{C}'$	(l',t')	$\mathcal{D}$
$[33,59,3]$	$[31,60,2]$	$(0,1)$	$[31,55,3]$	$(0,2)$	$[2,4,1]$
$[130,251,3]$	$[127,252,2]$	$(0,1)$	$[127,245,3]$	$(0,2)$	$[3,6,1]$
$[130,235,6]$	$[127,238,4]$	$(0,3)$	$[127,231,6]$	$(0,5)$	$[3,4,2]$
$[130,230,7]$	$[127,231,6]$	$(0,5)$	$[127,224,7]$	$(0,6)$	$[3,6,1]$
$[130,223,8]$	$[127,224,7]$	$(0,6)$	$[127,217,8]$	$(0,7)$	$[3,6,1]$
$[130,216,9]$	$[127,217,8]$	$(0,7)$	$[127,210,10]$	$(0,9)$	$[3,6,1]$
$[130,214,10]$	$[127,217,8]$	$(0,7)$	$[127,210,10]$	$(0,9)$	$[3,4,2]$
$[130,209,11]$	$[127,210,10]$	$(0,9)$	$[127,203,11]$	$(0,10)$	$[3,6,1]$
$[130,202,12]$	$[127,203,11]$	$(0,10)$	$[127,196,12]$	$(0,11)$	$[3,6,1]$
$[130,195,13]$	$[127,196,12]$	$(0,11)$	$[127,189,14]$	$(0,13)$	$[3,6,1]$
$[130,193,14]$	$[127,196,12]$	$(0,11)$	$[127,189,14]$	$(0,13)$	$[3,4,2]$
$[130,188,15]$	$[127,189,14]$	$(0,13)$	$[127,182,15]$	$(0,14)$	$[3,6,1]$
$[130,181,16]$	$[127,182,15]$	$(0,14)$	$[127,175,16]$	$(0,15)$	$[3,6,1]$
$[130,174,17]$	$[127,175,16]$	$(0,15)$	$[127,168,18]$	$(0,17)$	$[3,6,1]$
$[24,5,18]$	$[21,5,15]$	$(7,14)$	$[21,3,18]$	$(7,17)$	$[3,2,3]$
$[68,64,18]$	$[63,64,15]$	$(55,14)$	$[63,58,18]$	$(55,17)$	$[5,6,3]$
$[73,70,18]$	$[63,70,14]$	$(59,13)$	$[63,58,18]$	$(55,17)$	$[10,12,4]$
$[77,75,18]$	$[63,75,13]$	$(1,12)$	$[63,57,18]$	$(1,17)$	$[13,18,4]$
$[130,172,18]$	$[127,175,16]$	$(0,15)$	$[127,168,18]$	$(0,17)$	$[3,4,2]$
$[65,58,19]$	$[63,58,18]$	$(55,17)$	$[63,55,19]$	$(54,18)$	$[2,3,1]$
$[130,167,19]$	$[127,168,18]$	$(0,17)$	$[127,161,20]$	$(0,19)$	$[3,6,1]$
$[67,58,20]$	$[63,58,18]$	$(55,17)$	$[63,52,20]$	$(54,19)$	$[4,6,2]$
$[130,165,20]$	$[127,168,18]$	$(0,17)$	$[127,161,20]$	$(0,19)$	$[3,4,2]$
$[130,160,21]$	$[127,161,20]$	$(0,19)$	$[127,154,22]$	$(0,21)$	$[3,6,1]$
$[26,3,22]$	$[21,3,18]$	$(7,17)$	$[21,0,22]$	$(3,21)$	$[5,3,4]$
$[130,158,22]$	$[127,161,20]$	$(0,19)$	$[127,154,22]$	$(0,21)$	$[3,4,2]$
$[130,153,23]$	$[127,154,22]$	$(0,21)$	$[127,147,23]$	$(0,22)$	$[3,6,1]$
$[130,146,24]$	$[127,147,23]$	$(0,22)$	$[127,140,24]$	$(0,23)$	$[3,6,1]$
$[130,137,26]$	$[127,140,24]$	$(0,23)$	$[127,133,26]$	$(0,25)$	$[3,4,2]$
$[69,9,50]$	$[63,9,46]$	$(19,45)$	$[63,3,54]$	$(19,53)$	$[6,6,4]$
$[72,9,52]$	$[63,9,46]$	$(19,45)$	$[63,3,54]$	$(19,53)$	$[9,6,6]$
$[70,3,60]$	$[63,3,54]$	$(19,53)$	$[63,0,64]$	$(9,63)$	$[7,3,6]$
$[73,3,62]$	$[63,3,54]$	$(19,53)$	$[63,0,64]$	$(9,63)$	$[10,3,8]$
$[76,3,64]$	$[63,3,54]$	$(19,53)$	$[63,0,64]$	$(9,63)$	$[13,3,10]$

$\mathcal{E}$	$\bar{\mathcal{C}}$	(l,t)	$\mathcal{C}'$	(l',t')	$\mathcal{D}$
$[96,7,72]$	$[93,7,69]$	$(25,68)$	$[93,5,72]$	$(25,71)$	$[3,2,3]$
$[92,3,74]$	$[85,4,68]$	$(52,67)$	$[85,0,86]$	$(34,85)$	$[7,3,6]$
$[104,7,77]$	$[93,7,69]$	$(1,68)$	$[93,2,93]$	$(1,92)$	$[11,5,8]$
$[101,5,78]$	$[93,5,72]$	$(25,71)$	$[93,0,94]$	$(3,93)$	$[8,5,6]$
$[104,5,80]$	$[93,5,72]$	$(25,71)$	$[93,0,94]$	$(3,93)$	$[11,5,8]$
$[109,7,81]$	$[93,7,69]$	$(1,68)$	$[93,2,93]$	$(1,92)$	$[16,5,12]$
$[109,5,84]$	$[93,5,72]$	$(25,71)$	$[93,0,94]$	$(3,93)$	$[16,5,12]$
$[106,3,86]$	$[85,4,68]$	$(52,67)$	$[85,0,86]$	$(34,85)$	$[21,3,18]$
$[115,7,86]$	$[85,8,64]$	$(29,63)$	$[85,0,86]$	$(7,85)$	$[30,7,22]$
$[114,5,88]$	$[93,5,72]$	$(25,71)$	$[93,0,94]$	$(3,93)$	$[21,5,16]$
$[117,5,90]$	$[93,5,72]$	$(25,71)$	$[93,0,94]$	$(3,93)$	$[24,5,18]$
$[122,5,94]$	$[93,5,72]$	$(25,71)$	$[93,0,94]$	$(3,93)$	$[29,5,22]$

4.1.2 Konstruktion XX

$\mathcal{E}$	w	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[35,51,6]$	31	$1,2,52$	2	47	1	50	$0,5,45$	$0,5$	$[3,4,2]$	$[1,2,1]$
$[11,5,8]$	7	$1,4,5$	2	2	1	3	$0,7,0$	$0,7$	$[3,3,2]$	$[1,2,1]$
$[72,101,10]$	63	$1,5,102$	3	90	1	100	$0,9,88$	$0,9$	$[8,11,3]$	$[1,2,1]$
$[65,89,11]$	63	$1,8,90$	1	87	1	88	$0,10,85$	$0,10$	$[1,2,1]$	$[1,2,1]$
$[66,90,11]$	63	$1,8,90$	1	87	1	88	$0,10,85$	$0,10$	$[2,3,1]$	$[1,2,1]$
$[69,93,11]$	63	$1,6,96$	3	87	1	94	$0,10,85$	$0,10$	$[5,6,3]$	$[1,2,1]$
$[71,96,11]$	63	$1,6,96$	3	87	1	84	$0,10,85$	$0,10$	$[7,9,3]$	$[1,2,1]$
$[75,101,11]$	63	$1,5,102$	4	87	1	100	$0,10,85$	$0,10$	$[11,14,4]$	$[1,2,1]$
$[67,87,12]$	63	$1,9,87$	1	81	1	85	$0,11,79$	$0,11$	$[3,6,1]$	$[1,2,1]$
$[68,88,12]$	63	$55,9,88$	1	82	1	85	$54,11,79$	$54,11$	$[3,6,1]$	$[2,3,1]$
$[69,89,12]$	63	$1,8,90$	2	81	1	88	$0,11,79$	$0,11$	$[1,2,1]$	$[5,8,2]$
$[70,90,12]$	63	$1,8,90$	2	81	1	88	$0,11,79$	$0,11$	$[6,9,2]$	$[1,2,1]$
$[71,91,12]$	63	$57,7,94$	1	88	3	85	$54,11,79$	$54,11$	$[3,6,1]$	$[5,6,3]$
$[71,91,12]$	63	$57,7,94$	1	88	2	82	$54,11,79$	$54,11$	$[7,12,2]$	$[5,6,3]$
$[73,94,12]$	63	$57,7,94$	1	88	3	85	$54,11,79$	$54,11$	$[3,6,1]$	$[7,9,3]$
$[69,85,13]$	63	$54,10,85$	1	79	1	79	$53,12,73$	$53,12$	$[3,6,1]$	$[3,6,1]$
$[71,87,13]$	63	$1,9,87$	3	75	1	85	$0,13,73$	$0,13$	$[7,12,2]$	$[1,2,1]$
$[72,88,13]$	63	$55,9,88$	1	82	2	79	$53,12,73$	$53,12$	$[3,6,1]$	$[6,9,2]$
$[73,89,13]$	63	$55,8,90$	2	82	2	81	$53,12,73$	$55,12$	$[5,8,2]$	$[5,8,2]$
$[74,90,13]$	63	$55,8,90$	2	82	2	81	$53,12,73$	$55,12$	$[5,8,2]$	$[6,9,2]$
$[68,81,14]$	63	$1,10,81$	2	75	1	79	$0,13,73$	$0,13$	$[4,6,2]$	$[1,2,1]$
$[72,86,14]$	63	$1,9,87$	3	75	1	85	$0,13,73$	$0,13$	$[8,11,3]$	$[1,2,1]$
$[73,87,14]$	63	$1,9,87$	3	75	1	85	$0,13,73$	$0,13$	$[9,12,3]$	$[1,2,1]$
$[75,89,14]$	63	$1,8,90$	4	75	1	88	$0,13,73$	$0,13$	$[11,14,4]$	$[1,2,1]$
$[76,90,14]$	63	$1,8,90$	4	75	1	88	$0,13,73$	$0,13$	$[12,15,4]$	$[1,2,1]$
$[38,25,15]$	31	$21,11,25$	1	20	2	20	$19,14,15$	$19,15$	$[3,5,1]$	$[4,5,2]$
$[67,75,15]$	63	$1,12,75$	1	69	1	73	$0,14,67$	$0,14$	$[3,6,1]$	$[1,2,1]$
$[70,79,15]$	63	$53,11,79$	1	73	2	73	$51,14,67$	$51,14$	$[3,6,1]$	$[4,6,2]$
$[72,81,15]$	63	$53,10,81$	2	73	2	75	$51,14,67$	$51,14$	$[5,8,2]$	$[4,6,2]$

$\mathcal{E}$	w	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[74,84,15]$	63	$54,10,85$	1	79	3	73	$51,14,67$	$51,14$	$[3,6,1]$	$[8,11,3]$
$[75,85,15]$	63	$54,10,85$	1	79	3	73	$51,14,67$	$51,14$	$[3,6,1]$	$[9,12,3]$
$[76,86,15]$	63	$54,9,87$	2	79	3	75	$51,14,67$	$51,14$	$[5,8,2]$	$[8,11,3]$
$[77,87,15]$	63	$55,9,88$	1	82	4	73	$51,14,67$	$51,14$	$[3,6,1]$	$[11,14,4]$
$[69,73,16]$	63	$51,13,73$	1	67	1	67	$50,15,61$	$50,14$	$[3,6,1]$	$[3,6,1]$
$[71,75,16]$	63	$1,12,75$	2	63	1	73	$0,15,61$	$0,15$	$[7,12,2]$	$[1,2,1]$
$[74,79,16]$	63	$53,11,79$	2	67	2	73	$51,15,61$	$51,15$	$[7,12,2]$	$[4,6,2]$
$[69,67,17]$	63	$50,14,67$	1	61	1	61	$49,16,55$	$49,16$	$[3,6,1]$	$[3,6,1]$
$[73,73,17]$	63	$51,13,73$	1	67	2	61	$49,16,55$	$49,16$	$[3,6,1]$	$[7,12,2]$
$[75,75,17]$	63	$51,12,75$	2	67	2	63	$49,16,55$	$49,16$	$[5,8,2]$	$[7,12,2]$
$[71,67,18]$	63	$53,13,67$	2	61	2	61	$51,17,55$	$51,17$	$[4,6,2]$	$[4,6,2]$
$[69,63,19]$	63	$1,14,63$	3	57	1	61	$0,18,55$	$0,18$	$[5,6,3]$	$[1,2,1]$
$[70,64,19]$	63	$55,14,64$	3	58	1	61	$54,18,55$	$54,18$	$[5,6,3]$	$[2,3,1]$
$[74,69,19]$	63	$1,13,69$	4	57	1	67	$0,18,55$	$0,18$	$[10,12,4]$	$[1,2,1]$
$[75,70,19]$	63	$55,13,70$	4	58	1	67	$54,18,55$	$54,18$	$[10,12,4]$	$[2,3,1]$
$[65,56,20]$	63	$1,17,57$	1	54	1	55	$0,19,52$	$0,19$	$[1,2,1]$	$[1,2,1]$
$[66,57,20]$	63	$1,17,57$	1	54	1	55	$0,19,52$	$0,19$	$[2,3,1]$	$[1,2,1]$
$[71,61,20]$	63	$49,15,61$	1	55	3	55	$46,19,49$	$46,19$	$[3,6,1]$	$[5,6,3]$
$[40,7,30]$	31	$1,22,7$	8	2	1	5	$0,31,0$	$0,31$	$[8,5,6]$	$[1,2,1]$
$[66,31,30]$	63	$1,26,32$	2	29	1	30	$0,29,27$	$0,29$	$[2,2,2]$	$[1,2,1]$
$[43,7,32]$	31	$1,22,7$	8	2	1	5	$0,31,0$	$0,31$	$[11,5,8]$	$[1,2,1]$
$[66,10,48]$	63	$1,44,11$	2	8	1	9	$0,47,6$	$0,47$	$[2,2,2]$	$[1,2,1]$
$[67,11,48]$	63	$1,44,11$	2	8	1	9	$0,47,6$	$0,47$	$[3,3,2]$	$[1,2,1]$
$[72,7,54]$	63	$1,46,8$	16	2	1	6	$0,63,3$	$0,63$	$[8,5,6]$	$[1,2,1]$
$[83,5,64]$	63	$1,46,8$	16	2	1	6	$0,63,3$	$0,63$	$[19,3,16]$	$[1,2,1]$

ϕ $\mathbb{F}_4$-linear

$\mathcal{E}$	w	$l,t,k(l,t)$	i	$\tilde{k}_1$	j	$\tilde{k}_2$	$l',t',k(l',t')$	$(\tilde{l}',\tilde{t}')$	$\mathcal{D}_1$	$\mathcal{D}_2$
$[72,59,22]$	63	$1,14,60$	6	54	1	58	$0,21,52$	$0,21$	$[8,5,6]$	$[1,2,1]$
$[72,51,26]$	63	$1,21,52$	4	40	1	50	$0,26,38$	$0,26$	$[8,11,3]$	$[1,2,1]$
$[82,51,29]$	63	$22,21,52$	4	40	5	38	$17,30,26$	$17,30$	$[8,11,3]$	$[11,14,4]$
$[72,39,30]$	63	$1,25,40$	4	28	1	38	$0,30,26$	$0,30$	$[8,11,3]$	$[1,2,1]$
$[76,43,30]$	63	$21,23,44$	3	38	4	32	$17,30,26$	$17,30$	$[5,6,3]$	$[8,11,3]$
$[81,49,30]$	63	$21,22,50$	3	40	4	38	$17,30,26$	$17,30$	$[8,11,3]$	$[10,12,4]$
$[74,14,49]$	63	$22,42,14$	4	8	5	6	$17,51,0$	$17,63$	$[6,6,4]$	$[5,8,2]$
$[75,13,50]$	63	$22,42,14$	4	8	5	6	$17,51,0$	$17,63$	$[6,6,4]$	$[6,7,3]$
$[80,13,53]$	63	$22,42,14$	4	8	5	6	$17,51,0$	$17,63$	$[7,5,5]$	$[10,8,6]$

4.1.3 Konstruktion X^3

$w = 63$

$\mathcal{E}$	l_1, t_1, k_1	l_2, t_2, k_2	l_3, t_3, k_3	l'_1, t'_1, k'_1	d'_2, k'_2	d'_3, k'_3	$\mathcal{D}_1$	$\mathcal{D}_2$	$\mathcal{D}_3$
$[73, 98, 11]$	$1, 5, 102$	$1, 6, 96$	$1, 9, 87$	$0, 6, 100$	$8, 94$	$11, 85$	$[1, 2, 1]$	$[1, 2, 1]$	$[8, 11, 3]$
$[70, 83, 14]$	$1, 9, 87$	$1, 10, 81$	$1, 12, 75$	$0, 10, 85$	$12, 79$	$14, 73$	$[1, 2, 1]$	$[1, 2, 1]$	$[5, 8, 2]$
$[76, 71, 19]$	$1, 12, 75$	$1, 13, 69$	$1, 17, 57$	$0, 13, 73$	$15, 67$	$19, 55$	$[1, 2, 1]$	$[1, 2, 1]$	$[11, 14, 4]$
$[83, 10, 60]$	$19, 44, 11$	$17, 46, 8$	$1, 62, 2$	$19, 45, 9$	$48, 6$	$64, 0$	$[1, 2, 1]$	$[2, 2, 2]$	$[17, 8, 12]$

$w = 63$ ϕ **$\mathbb{F}_4$-linear**

$\mathcal{E}$	l_1, t_1, k_1	l_2, t_2, k_2	l_3, t_3, k_3	l'_1, t'_1, k'_1	d'_2, k'_2	d'_3, k'_3	$\mathcal{D}_1$	$\mathcal{D}_2$	$\mathcal{D}_3$
$[71, 47, 27]$	$1, 21, 52$	$1, 22, 46$	$1, 25, 40$	$0, 22, 50$	$24, 44$	$27, 38$	$[1, 2, 1]$	$[1, 1, 1]$	$[6, 7, 3]$
$[80, 54, 28]$	$1, 20, 54$	$1, 21, 52$	$1, 25, 40$	$62, 22, 46$	$24, 44$	$28, 32$	$[5, 8, 2]$	$[1, 2, 1]$	$[11, 14, 4]$
$[77, 46, 29]$	$1, 22, 46$	$0, 23, 44$	$59, 27, 32$	$1, 25, 40$	$27, 38$	$31, 26$	$[5, 6, 3]$	$[1, 2, 1]$	$[8, 14, 2]$
$[82, 52, 29]$	$0, 21, 52$	$0, 22, 50$	$0, 26, 38$	$59, 25, 40$	$27, 38$	$31, 26$	$[7, 12, 2]$	$[1, 2, 1]$	$[11, 14, 4]$
$[71, 35, 31]$	$1, 25, 40$	$1, 26, 34$	$1, 29, 28$	$0, 26, 38$	$28, 32$	$31, 26$	$[1, 2, 1]$	$[1, 1, 1]$	$[6, 7, 3]$
$[80, 46, 31]$	$1, 22, 46$	$0, 23, 44$	$59, 27, 32$	$1, 25, 40$	$27, 38$	$31, 26$	$[5, 6, 3]$	$[1, 2, 1]$	$[11, 14, 4]$
$[71, 15, 47]$	$1, 41, 16$	$1, 42, 14$	$1, 46, 8$	$0, 42, 14$	$44, 12$	$48, 6$	$[1, 2, 1]$	$[1, 1, 1]$	$[6, 7, 3]$
$[75, 14, 50]$	$0, 42, 14$	$0, 43, 12$	$0, 47, 6$	$59, 46, 8$	$48, 6$	$64, 0$	$[6, 6, 4]$	$[1, 2, 1]$	$[5, 8, 2]$
$[76, 13, 51]$	$0, 42, 14$	$0, 43, 12$	$0, 47, 6$	$59, 46, 8$	$48, 6$	$64, 0$	$[6, 6, 4]$	$[1, 1, 1]$	$[6, 7, 3]$

Ist die Dimension bzw die Codimension obiger Codes sehr klein, so haben diese Codes meist mehr Codeworte als ein linearer Code haben kann. Ist hingegen die Dimension in der Nähe der Länge, so haben obige Codes oft sehr viel mehr Codeworte als ein bekannter linearer Code, obwohl sie noch unter der oberen Schranke der linearen Codes liegen. Ein extremes Beispiel ist der additive $[128, 191, 14]$.Der laut Datenbank best bekannte lineare quaternäre Code ist ein $[128, 91, 14]$. Der $[128, 191, 14]$ hat also die $2^9 = 512$ fache Anzahl von Codeworten.

4.2 Konkatenation

In diesem Abschnitt werden wir als erstes sehen, daß man durch Konkatenation (Bemerkung 1.19) mit einem linearen, q-ären Code, aus q^u-ären $\mathbb{F}_q$-linearen Codes lineare, q-äre Codes bekommt. Dann werden wir dies im Fall quaternärer $\mathbb{F}_2$-linearer Codes zur Konstruktion neuer linearer, binärer Codes verwenden. Aus den bisher von uns gefundenen linearen, quaternären Codes liefert nur einer durch Konkatenation einen neuen linearen, binären Code: der quaternäre $[53, 6, 36]$ (aus Konstruktion XX) liefert durch Konkatenation mit dem linearen, binären $[3, 2, 2]$ einen linearen, binären $[159, 12, 72]$.

Bemerkung 4.2 *Sei $\mathcal{A}$ ein q^u-ärer, $\mathbb{F}_q$-linearer $[n, k, d]$, $\mathcal{B}$ ein linearer, q-ärer $[n', u, d']$. Dann kann man die Konkatenation so einrichten, daß der konkatenierte Code ein linearer, q-ärer $[nn', k, dd']$ ist.*

Beweis: Man beachte, daß beim $\mathbb{F}_q$-linearen Code $\mathcal{A}$ k die Dimension k über $\mathbb{F}_q$ zu nehmen ist. Das Alphabet von $\mathcal{A}$ ist ein u-dimensionaler $\mathbb{F}_q$-Vektorraum ebenso der Code $\mathcal{B}$. Sei $\psi : \mathcal{A} \to \mathcal{B}$ ein Vektorraumisomorphismus. Bemerkung 1.19 liefert die Behauptung bis auf die Linearität. Wählt man für die Abbildung im Beweis von Bemerkung 1.19 obiges ψ, so ist der konkatenierte Code linear ■

Sei ϕ wie in Abschnitt 4.1 gewählt. Wir werden für unsere Konstruktionen folgende Codes $\mathcal{C}(63, l, t)$ verwenden:

$$\begin{aligned}
\mathcal{C}(1,44) = [63,11,45], \quad \mathcal{C}(1,46) = [63,8,47], \quad \mathcal{C}(1,62) = [63,2,63],\\
\mathcal{C}(0,45) = [63,9,46], \quad \mathcal{C}(0,47) = [63,6,48], \quad \mathcal{C}(0,63) = [63,0,64],\\
\mathcal{C}(19,45) = [63,9,46], \quad \mathcal{C}(19,53) = [63,3,54],\\
\mathcal{C}(17,47) = [63,6,48], \quad \mathcal{C}(17,55) = [63,0,64].
\end{aligned}$$

Nach dem Konkatenieren mit den linearen, binären $[3,2,2]$ erhalten wir die folgenden linearen, binären Codes

$$\begin{aligned}
\mathcal{C}_1 = [189,11,90], \quad \mathcal{C}_2 = [189,8,94], \quad \mathcal{C}_3 = [189,2,126],\\
\mathcal{C}_4 = [189,9,92], \quad \mathcal{C}_5 = [189,6,96], \quad \mathcal{C}_6 = [189,0,190],\\
\mathcal{C}_a = [189,9,92], \quad \mathcal{C}_b = [189,3,108], \quad \mathcal{C}_c = [189,6,96], \quad \mathcal{C}_d = [189,0,190].
\end{aligned}$$

Dabei übertragen sich die Teilcodebeziehungen der quaternären Ausgangscodes (vergleiche Bemerkung 2.14) und man hat somit $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$, $\mathcal{C}_4 \supset \mathcal{C}_5 \supset \mathcal{C}_6$, $\mathcal{C}_1 \supset \mathcal{C}_4$ und $\mathcal{C}_i \cap \mathcal{C}_{i+2} = \mathcal{C}_{i+3}$ für $i = 2, 3$. Sowie $\mathcal{C}_a \supset \mathcal{C}_b, \mathcal{C}_c$ und $\mathcal{C}_b \cap \mathcal{C}_c = \mathcal{C}_d$.

Schon $\mathcal{C}_1 = [189, 11, 90]$ ist neu und optimal. Nach Bemerkung (1.12) folgt aus der Existenz eines $\mathbb{F}_2$-linearen, quaternären $[n, k, d]$ die Existenz eines $[n-1, k-2, d]$ und eines $[n-1, k, d-1]$. Damit erhalten wir ausgehend von $\mathcal{C}(1, 44) = [63, 11, 45]$ und anschließender Konkatenation folgende lineare, binäre Codes

$$\begin{aligned}
&[186,11,88],\ [183,11,86],\ [180,11,84],\\
&[177,11,82],\ [171,11,78],\ [186,9,90].
\end{aligned}$$

Der $[186, 11, 88]$ und $[186, 9, 90]$ sind optimal. Der Code $\mathcal{C}_1$ hat ein Wort vom Gewicht 96, der $[186, 11, 88]$ ein Wort vom Gewicht 108. Wenden wir Satz 1.13 mit diesen Worten an, so erhalten wir einen linearen, binären

$$[93, 10, 42] \text{ bzw. } [78, 10, 34].$$

Konstruktion X (Bemerkung 1.17) auf $\mathcal{C}_1$, $\mathcal{C}_4$ mit Hilfscode $[3, 2, 2]$ angewandt, liefert einen

$$[192, 11, 92].$$

Dieser ist optimal und hat die Gewichtsverteilung

$$A_0 = 1, A_{92} = 1344, A_{96} = 252, A_{108} = 448, A_{128} = 3.$$

Wenden wir Satz 1.13 mit einem Wort vom Gewicht 96 bzw. 108 an, so erhalten wir die neuen und optimalen Codes

$$[96, 10, 44] \text{ bzw. } [84, 10, 38].$$

Wenden wir Satz 1.13 mit einem Wort vom Gewicht 128 an, so liefert dies einen $[64, 10, 28]$. Dieser ist optimal aber bekannt. Desweiteren erhalten wir aus Konstruktion X die optimalen Codes:

$$\begin{array}{lll} [196, 11, 94] & \text{aus } \mathcal{C}_1, \mathcal{C}_2 \text{ mit} & [7, 3, 4], \\ [193, 9, 94] & \text{aus } \mathcal{C}_4, \mathcal{C}_5 \text{ mit} & [4, 3, 2], \\ [196, 9, 96] & \text{aus } \mathcal{C}_4, \mathcal{C}_5 \text{ mit} & [7, 3, 4], \\ [221, 9, 108] & \text{aus } \mathcal{C}_a, \mathcal{C}_b \text{ mit} & [32, 6, 16]. \end{array}$$

Aus dem $[196, 11, 94]$ erhalten wir nach einem Griesmerschritt (Bemerkung 1.14) einen optimalen

$$[100, 10, 46].$$

Wir erhalten aus $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_4$ und $\mathcal{C}_5$ durch Konstruktion XX (Bemerkung 1.18) mit den Hilfscodes $[3, 2, 2]$ und $[7, 3, 4]$ einen optimalen

$$[199, 11, 96].$$

Außerdem hat der $[199, 11, 96]$ ein Wort vom Gewicht 112. Wendet man Satz 1.13 mit diesem Wort bzw. einem Wort vom Gewicht 96 (Griesmerschritt) an, so erhält man die neuen und optimalen Codes

$$[87, 10, 40] \text{ bzw. } [103, 10, 48].$$

Ebenfalls mit Konstruktion XX erhalten wir aus $\mathcal{C}_a$, $\mathcal{C}_b$, $\mathcal{C}_c$ und $\mathcal{C}_d$ einen:

$$\begin{array}{lll} [203, 9, 98] & \text{mit den Hilfscodes} & [7, 3, 4] \text{ und } [7, 6, 2], \\ [211, 9, 102] & \text{mit den Hilfscodes} & [7, 3, 4] \text{ und } [15, 6, 6], \\ [214, 9, 104] & \text{mit den Hilfscodes} & [7, 3, 4] \text{ und } [18, 6, 8], \\ [228, 9, 112] & \text{mit den Hilfscodes} & [7, 3, 4] \text{ und } [32, 6, 16]. \end{array}$$

Diese sind bis auf den $[211, 9, 102]$ optimal. Benutzt man als Codes für Konstruktion X^3 (Satz 3.5) $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ und setzt $\mathcal{C}' = \mathcal{C}_4$, so ist $\mathcal{C}_2 \cap \mathcal{C}' = \mathcal{C}_5$ und $\mathcal{C}_3 \cap \mathcal{C}' = \mathcal{C}_6$. Mit den Hilfscodes $\mathcal{D}_1$, $\mathcal{D}_2$ und $\mathcal{D}_3$ erhält man :

$$\begin{array}{lll} [246, 9, 120] & \text{mit} & \mathcal{D}_1 = [3, 2, 2], \mathcal{D}_2 = [4, 1, 4] \text{ und } \mathcal{D}_3 = [50, 7, 24], \\ [246, 10, 118] & \text{mit} & \mathcal{D}_1 = [3, 2, 2], \mathcal{D}_2 = [6, 2, 4] \text{ und } \mathcal{D}_3 = [48, 8, 22], \\ [249, 10, 120] & \text{mit} & \mathcal{D}_1 = [3, 2, 2], \mathcal{D}_2 = [6, 2, 4] \text{ und } \mathcal{D}_3 = [51, 8, 24]. \end{array}$$

5 BCH-Codes über großen Körpern

In diesem Abschnitt werden wir BCH-Codes über größeren Körpern benutzen, um wie in Abschnitt 4.2, nach Konkatenation, mit den diversen Konstruktionen neue binäre und ternäre Codes zu erhalten. Die meisten dieser Codes haben eine größere Länge als durch die Datenbank abgedeckt. Dann werden wir einen Griesmerschritt (Bemerkung 1.14) bzw. Satz 1.13 benutzen, um in den Bereich der Datenbank zu gelangen. Dabei ist zu erwähnen, daß es meist mehrere verschiedene lange Codes gibt, die denselben kürzeren liefern. Von diesen werden wir nur einen konstruieren. Wir werden hier nur solche Konstruktionen erwähnen, die zu neuen Codes führen. Man erhält aber mit diesem Verfahren auch noch viele lange Codes, die nach Reduktion auf datenbankgerechte Länge einen optimalen oder bestbekannten Code liefern. Dieses Verfahren liefert nur für kleine Dimensionen gute Ergebnisse.

Wir verwenden die folgenden quaternären, linearen $\mathcal{B}(63, l, t)$ Codes:

$$\begin{array}{lll} \mathcal{B}(1,41) = [63,8,42], & \mathcal{B}(1,42) = [63,7,43], & \mathcal{B}(1,46) = [63,4,47], \\ \mathcal{B}(0,42) = [63,7,43], & \mathcal{B}(0,43) = [63,6,44], & \mathcal{B}(0,47) = [63,3,48]. \end{array}$$

Nach Konkatenation mit den linearen, binären $[3,2,2]$ erhalten wir die folgenden linearen, binären Codes:

$$\begin{array}{lll} \mathcal{C}_1 = [189,16,84], & \mathcal{C}_2 = [189,14,86], & \mathcal{C}_3 = [189,8,94], \\ \mathcal{C}_4 = [189,14,86], & \mathcal{C}_5 = [189,12,88], & \mathcal{C}_6 = [189,6,96]. \end{array}$$

Dabei übertragen sich die Teilcodebeziehungen der quaternären Codes (vergleiche Bemerkung 2.14) und man hat somit $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$, $\mathcal{C}_4 \supset \mathcal{C}_5 \supset \mathcal{C}_6$, $\mathcal{C}_1 \supset \mathcal{C}_4$ und $\mathcal{C}_i \cap \mathcal{C}_{i+2} = \mathcal{C}_{i+3}$ für $i = 2, 3$.

Wenden wir Konstruktion X auf $\mathcal{C}_2, \mathcal{C}_3$ mit dem Hilfscode $[16,5,8]$ an, so erhalten wir einen

$$[205, 13, 94].$$

Benutzt man als Codes für Konstruktion X^3 (Satz 3.5) $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ und setzt $\mathcal{C}' = \mathcal{C}_4$, so ist $\mathcal{C}_2 \cap \mathcal{C}' = \mathcal{C}_5$ und $\mathcal{C}_3 \cap \mathcal{C}' = \mathcal{C}_6$. Mit den Hilfscodes $\mathcal{D}_1 = [3,2,2]$, $\mathcal{D}_2 = [2,1,2]$ und $\mathcal{D}_3$ erhält man :

$$\begin{array}{lll} [202,15,90] & \text{mit} & \mathcal{D}_3 = [8,7,2], \\ [206,15,92] & \text{mit} & \mathcal{D}_3 = [12,7,4], \\ [210,15,94] & \text{mit} & \mathcal{D}_3 = [16,7,6], \\ [213,15,96] & \text{mit} & \mathcal{D}_3 = [19,7,8]. \end{array}$$

Desweiteren haben wir $\mathcal{B}(1,21) = [63,26,22] \supset \mathcal{B}(1,25) = [63,20,26], \mathcal{B}(0,22) = [63,25,23]$ und $\mathcal{B}(1,25) \cap B(0,22) = \mathcal{B}(0,26) = [63,19,27]$. Nach Konkatenation liefert Konstruktion XX mit den binären Hilfscodes $[3,2,2]$ und $[24,12,8]$ einen

$$[216,52,54].$$

Wir verwenden die folgenden 8-ären, linearen $\mathcal{B}(63,l,t)$ Codes:

$$\begin{array}{lll} \mathcal{B}(1,53) = [63,4,54], & \mathcal{B}(1,54) = [63,3,55], & \mathcal{B}(1,62) = [63,1,63], \\ \mathcal{B}(0,54) = [63,3,55], & \mathcal{B}(0,55) = [63,2,56], & \mathcal{B}(0,63) = [63,0,64]. \end{array}$$

Nach Konkatenation mit den linearen, binären $[7,3,4]$ erhalten wir die folgenden linearen, binären Codes:

$$\begin{array}{lll} \mathcal{C}_1 = [441,12,216], & \mathcal{C}_2 = [441,9,220], & \mathcal{C}_3 = [441,3,252], \\ \mathcal{C}_4 = [441,9,220], & \mathcal{C}_5 = [441,6,224], & \mathcal{C}_6 = [441,0,442]. \end{array}$$

Dabei übertragen sich die Teilcodebeziehungen aus dem 8-ären und man hat somit $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$, $\mathcal{C}_4 \supset \mathcal{C}_5 \supset \mathcal{C}_6$, $\mathcal{C}_1 \supset \mathcal{C}_4$ und $\mathcal{C}_i \cap \mathcal{C}_{i+2} = \mathcal{C}_{i+3}$ für $i = 2,3$.

Da $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_5$, enthält $\mathcal{C}_1$ Worte vom Gewicht 220 und 224. (Berechnet man die Gewichtsverteilung, so sieht man, daß die Teilcodes die genannten Distanzen als Minimaldistanzen haben). Wendet man Satz 1.13 auf $\mathcal{C}_1$ mit diesen Worten an, so erhält man einen optimalen

$$[221,11,106] \text{ bzw. } [217,11,104].$$

Ein weiterer Griesmerschritt liefert aus dem $[221,11,106]$ einen

$$[109,10,50].$$

Nehmen wir von den 8-ären $\mathcal{B}(1,53)$ die Teilcodes, die alle bis auf i Koordinaten enthalten, so erhält man nach der Konkatenation einen $[441-7i, 12, 216-4i]$. Für i=1 enthält der Code unter anderem Worte vom Gewicht 220 und 224. Satz 1.13 mit diesen Worten liefert einen

$$[214,11,102] \text{ bzw. } [210,11,100].$$

Für i=2 gibt es unter anderem Worte vom Gewicht 220. Satz 1.13 mit diesem Wort liefert einen

$$[207,11,98].$$

Wendet man Konstruktion X auf $\mathcal{C}_1$, $\mathcal{C}_4$ mit Hilfscode $[7,3,4]$ an, so bekommt man einen $[448,12,220]$ und nach einem Griesmerschritt einen optimalen

$$[228,11,110].$$

Die Gewichtsverteilung des $[448,12,220]$ ist

$$A_0 = 1, A_{220} = 3136, A_{224} = 504, A_{252} = 448, A_{256} = 7.$$

Wendet man Satz 1.13 mit einem Wort vom Gewicht 224 an, so erhält man einen optimalen

$$[224,11,108].$$

Satz 1.13 angewandt mit Worten vom Gewicht 252 bzw. 256 liefert einen $[196,11,94]$ bzw. $[196,11,92]$. Diese sind schon in Abschnitt 4.2 konstruiert worden. Die Gewichtsverteilung des $[224,11,108]$ ist

$$A_0 = 1, A_{108} = 1372, A_{112} = 248, A_{124} = 392, A_{128} = 7, A_{140} = 28.$$

Wendet man Satz 1.13 mit Worten vom Gewicht 108 bzw. 112 an, so erhält man einen

$$[116,10,54] \text{ bzw. } [112,10,52]$$

Wendet man die iterierte Konstruktion X auf die Codes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ mit den Hilfscodes $[6,2,4]$, $[51,8,24]$ an, so erhält man einen $[498,11,244]$ und nach einem Griesmerschritt einen

$$[254,10,122].$$

Wendet man die Konstruktion XX auf die Codes $\mathcal{C}_1 \supset \mathcal{C}_2, \mathcal{C}_4 \supset \mathcal{C}_5$ mit den Hilfscodes $[7,3,4]$ und $[7,3,4]$ an, so erhält man einen $[455,12,224]$ und nach einem bzw. zwei Griesmerschritten die optimalen Codes

$$[231,11,112] \text{ bzw. } [119,10,56].$$

Benutzt man als Codes für Konstruktion X^3 $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ und setze $\mathcal{C}' = \mathcal{C}_4$, so ist $\mathcal{C}_2 \cap \mathcal{C}' = \mathcal{C}_5$ und $\mathcal{C}_3 \cap \mathcal{C}' = \mathcal{C}_6$. Mit den Hilfscodes $\mathcal{D}_1 = [7,3,4]$, $\mathcal{D}_2$ und $\mathcal{D}_3$ erhält man :

$$
\begin{array}{llll}
\mathcal{D}_2 = [4,1,4],\ \mathcal{D}_3 = [8,7,2] & \text{einen} & [460,10,226] \xrightarrow{G} [234,9,113], \\
\mathcal{D}_2 = [6,2,4],\ \mathcal{D}_3 = [9,8,2] & \text{einen} & [463,11,226] \xrightarrow{G} [237,10,113], \\
\mathcal{D}_2 = [6,2,4],\ \mathcal{D}_3 = [20,8,8] & \text{einen} & [474,11,232] \xrightarrow{G} [242,10,116], \\
\mathcal{D}_2 = [6,2,4],\ \mathcal{D}_3 = [51,8,24] & \text{einen} & [505,11,248] \xrightarrow{G} [257,10,124], \\
\mathcal{D}_2 = [7,3,4],\ \mathcal{D}_3 = [10,9,2] & \text{einen} & [465,12,226] \xrightarrow{G} [239,11,113], \\
\mathcal{D}_2 = [7,3,4],\ \mathcal{D}_3 = [21,9,8] & \text{einen} & [476,12,232] \xrightarrow{G} [244,11,116], \\
\mathcal{D}_2 = [7,3,4],\ \mathcal{D}_3 = [30,9,12] & \text{einen} & [485,12,236] \xrightarrow{G} [249,11,118], \\
\mathcal{D}_2 = [7,3,4],\ \mathcal{D}_3 = [47,9,20] & \text{einen} & [502,12,244] \xrightarrow{G} [258,11,122].
\end{array}
$$

Dabei ist $\xrightarrow{G}$ als, „nach Anwendung eines Griesmerschrittes erhält man“, zu lesen.

Wir verwenden die folgenden 9-ären, linearen $\mathcal{B}(80,l,t)$ Codes:

$$
\begin{array}{lll}
\mathcal{B}(1,69) = [80,4,70], & \mathcal{B}(1,70) = [80,3,71], & \mathcal{B}(1,79) = [80,1,80], \\
\mathcal{B}(0,70) = [80,3,71], & \mathcal{B}(0,71) = [80,2,72], & \mathcal{B}(0,80) = [80,0,81].
\end{array}
$$

Nach Konkatenation mit den linearen, ternären $[4,2,3]$ erhalten wir die folgenden linearen, ternären Codes

$$
\begin{array}{lll}
\mathcal{C}_1 = [320,8,210], & \mathcal{C}_2 = [320,6,213], & \mathcal{C}_3 = [320,2,240], \\
\mathcal{C}_4 = [320,6,213], & \mathcal{C}_5 = [320,3,216], & \mathcal{C}_6 = [320,0,321].
\end{array}
$$

Wie oben übertragen sich die Teilcodebeziehungen der 9-ären Codes und man hat somit $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$, $\mathcal{C}_4 \supset \mathcal{C}_5 \supset \mathcal{C}_6$, $\mathcal{C}_1 \supset \mathcal{C}_4$ und $\mathcal{C}_i \cap \mathcal{C}_{i+2} = \mathcal{C}_{i+3}$ für $i = 2,3$.

$\mathcal{C}_1$ enthält ein Wort vom Gewicht 216, Satz 1.13 liefert einen

$$[104,7,66].$$

Streicht man aus $\mathcal{B}(1,69)$ eine Spalte, so erhält man nach der Konkatenation einen $[316,8,207]$. Dieser enthält ein Wort vom Gewicht 216. Satz 1.13 liefert einen optimalen

$$[100,7,63].$$

Wendet man auf $\mathcal{C}_1, \mathcal{C}_2$ Konstruktion X mit Hilfscode $[4,2,3]$ an, so erhält man einen $[327,8,213]$. Dieser enthält ein Wort vom Gewicht 216. Satz 1.13 liefert einen optimalen

$$[108,7,69].$$

Wendet man die Konstruktion XX auf die Codes $\mathcal{C}_1 \supset \mathcal{C}_2, \mathcal{C}_4 \supset \mathcal{C}_5$ mit den Hilfscodes $[4, 2, 3]$ und $[4, 2, 3]$ an, so erhält man einen $[328, 8, 216]$ und nach einem Griesmerschritt einen optimalen

$$[112, 7, 72].$$

Benutzt man als Codes für Konstruktion X^3 $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ und setze $\mathcal{C}' = \mathcal{C}_4$, so ist $\mathcal{C}_2 \cap \mathcal{C}' = \mathcal{C}_5$ und $\mathcal{C}_3 \cap \mathcal{C}' = \mathcal{C}_6$. Mit den Hilfscodes $\mathcal{D}_1 = \mathcal{D}_2 = [4, 2, 3]$ und $\mathcal{D}_3$ erhält man :

$$\begin{array}{lll}
\mathcal{D}_3 = [12, 6, 6] & \text{einen} & [340, 8, 222] \xrightarrow{G} [118, 7, 74], \\
\mathcal{D}_3 = [15, 6, 7] & \text{einen} & [343, 8, 223] \xrightarrow{G} [120, 7, 75], \\
\mathcal{D}_3 = [26, 6, 15] & \text{einen} & [354, 8, 231] \xrightarrow{G} [123, 7, 77].
\end{array}$$

6 Verlängerungen von BCH-Codes

In diesem Abschnitt werden die Ergebnisse der Suche nach Verlängerungen, von einigen BCH-Codes kleiner Distanz und kleiner Codimension, mit dem Computer präsentiert. Dabei verstehen wir unter Verlängern eines $[n, k, d]$, genauer unter Verlängern seiner Checkmatrix, um x Spalten, analog wie im Beweis von Satz 1.22 verwendet, folgendes: Es gibt x Vektoren $\in \mathbb{F}_q^{n-k}$, so daß in der Matrix, die man erhält wenn man diese Vektoren als Spalten zu der Checkmatrix des $[n, k, d]$ hinzufügt, immer noch je $d-1$ Spalten linear unabhängig sind (sie also eine Checkmatrix eines $[n+x, k+x, d]$ ist). Als weitere Konstruktion werden wir, analog zu der Idee von Satz 1.24, der Checkmatrix eine Nullzeile hinzufügen und diese Matrix dann verlängern. Wir erhalten somit aus einem $[n, k, d]$ und x zusätzlichen Spalten einen $[n+x, k-1+x, d]$.

In den Sätze 1.22 und 1.24 werden nur die Parameter eines Codes verwendet um Aussagen über dessen Verlängerbarkeit zu machen. Es ist also nicht weiter verwunderlich, daß man meist bessere Verlängerungen finden kann. Als Beispiel nehmen wir das erste unten aufgeführte Ergebnis: Mit dem Computer ließ sich eine Verlängerung des erweiterten BCH-Codes (siehe Bemerkung 2.28) $\hat{\mathcal{B}}(127, 1, 6) = [128, 106, 7]$ um 26 Spalten finden. Durch Satz 1.22 wird in diesem Fall keine Verlängerung garantiert.

Die Checkmatrizen der verlängerten Codes sind in Anhang B zu finden. Man erhält:

für q=2

$[154, 132, 7]$	aus	$[128, 106, 7]^\perp$	$=\hat{\mathcal{B}}(127, 1, 6)^\perp$	+ 26 Spalten
$[161, 138, 7]$	aus	$[154, 132, 7]^\perp$	+ Nullzeile	+ 7 Spalten
$[71, 46, 9]$	aus	$[64, 39, 9]^\perp$	$=\hat{\mathcal{B}}(63, 1, 8)^\perp$	+ 7 Spalten
$[38, 12, 13]$	aus	$[32, 6, 13]^\perp$	$=\hat{\mathcal{B}}(31, 1, 12)^\perp$	+ 6 Spalten

für q=4

$[87, 78, 5]$	aus	$[65, 57, 5]^\perp$	von Seite 51 + Nullzeile	+ 21 Spalten
$[145, 135, 5]$	aus	$[87, 78, 5]^\perp$	+ Nullzeile	+ 57 Spalten
$[70, 57, 7]$	aus	$[64, 51, 7]^\perp$	$=\hat{\mathcal{B}}(63, 1, 6)^\perp$	+ 6 Spalten

für q=3

$[86, 77, 5]$	aus	$[81, 72, 5]^{\perp}$	$=\hat{\mathcal{B}}(80, 1, 4)^{\perp}$	+ 5 Spalten
$[134, 123, 5]$	aus	$[122, 111, 5]^{\perp}$	$=\hat{\mathcal{B}}(121, 1, 4)^{\perp}$	+ 12 Spalten
$[33, 21, 7]$	aus	$[26, 14, 7]^{\perp}$	$=\mathcal{B}(26, 1, 7)^{\perp}$	+ 7 Spalten
$[42, 29, 7]$	aus	$[33, 21, 7]^{\perp}$	+ Nullzeile	+ 9 Spalten
$[52, 38, 7]$	aus	$[42, 29, 7]^{\perp}$	+ Nullzeile	+ 10 Spalten
$[92, 76, 7]$	aus	$[85, 70, 7]^{\perp}$	von Seite 51 + Nullzeile	+ 7 Spalten
$[108, 91, 7]$	aus	$[92, 76, 7]^{\perp}$	+ Nullzeile	+ 16 Spalten
$[34, 20, 8]$	aus	$[27, 14, 8]^{\perp}$	$=\hat{\mathcal{B}}(26, 1, 7)^{\perp}$ + Nullzeile	+ 9 Spalten
$[44, 29, 8]$	aus	$[41, 26, 8]^{\perp}$	$=\hat{\mathcal{B}}(40, 1, 7)^{\perp}$	+ 3 Spalten
$[25, 10, 10]$	aus	$[21, 6, 10]^{\perp}$	$=\hat{\mathcal{B}}(20, 1, 9)^{\perp}$	+ 4 Spalten

Dabei sind die binären $[155, 132, 8]$, $[162, 138, 8]$, $[38, 12, 13]$ und der ternäre $[86, 77, 5]$ optimal. Auch einige duale Codes liefern gute Parameter:

$q = 3$

Der duale Code des $\hat{\mathcal{B}}(80, 1, 44) = [81, 11, 45]$ ist ein $[81, 70, 6]$. Dessen dualer Code (also der $\hat{\mathcal{B}}(80, 1, 44)$) läßt sich um 4 Spalten verlängern. Man erhält so einen optimalen

$$[85, 74, 6],$$

dieser hat duale Distanz 46. Konstruktion Y1 (1.20) liefert einen optimalen

$$[39, 29, 6].$$

Die Checkmatrix des $[85, 74, 6]$ ergänzt um eine Nullzeile läßt sich um 10 Spalten verlängern. Ergänzt man dies Matrix wiederum um eine Nullzeile so läßt sie sich nochmals um 8 Spalten verlängern. Um eine weitere Nullzeile ergänzt kann man die Matrix nochmals um 13 Spalten verlängern. Wir erhalten somit folgend Codes:

$$[95, 83, 6],\ [103, 90, 6],\ [116, 102, 6].$$

Die ersten 72 Spalten der angegebenen Checkmatrix des $[86, 77, 5]$ sind die Erzeugermatrix eines

$$[72, 9, 40].$$

Der duale Code des $[86, 77, 5]$ ist ein

$$[86, 9, 50].$$

$q = 4$

Es ist $\hat{\mathcal{B}}(63, 1, 32) = [64, 8, 33] \subset \hat{\mathcal{B}}(63, 1, 31) = [64, 11, 32]$ und läßt sich somit (durch Konstruktion X) um 3 Spalten erweitern. Wir bekommen also einen $[67, 11, 33]$. Dessen dualer ist ein $[67, 56, 6]$. Dessen dualer Code (also der erweiterte $\hat{\mathcal{B}}(63, 1, 32)$) läßt sich um 14 Spalten verlängern, man erhält also einen

$$[81, 70, 6].$$

Die Checkmatrix des $[81, 70, 6]$ ergänzt um eine Nullzeile läßt sich um 25 Spalten verlängern. wir erhalten somit einen

$$[106, 94, 6].$$

Die Einschränkung der Checkmatrix des $\mathcal{B}(63, 1, 5) = [63, 51, 6]$ auf geeignete 43 Koordinaten ist eine Erzeugermatrix eines

$$[43, 12, 19].$$

Konklusion

Als Anwendung der verallgemeinerten BCH-Codes und des hier gewählten Zugangs zu diesen, haben wir in dieser Arbeit nur neue Codes konstruiert. Da es aber vielfältige Beziehungen der Codierungstheorie zu anderen Gebieten der Mathematik gibt ist zu hoffen, daß man aus dieser Arbeit weiteren Nutzen ziehen kann. Einige Auswirkungen die in andere Gebiete hineinreichen gibt es bereits.

In den folgenden Fällen führten die vielen hier konstruierten neuen Codes (vorsichtig geschätzt wurden gut 5% der Einträge der Datenbank [8] verbessert) zu Verbesserungen in den Anwendungen:

W.Schmid und R.Wolf haben in [26], neue Schranken für digitale Netze konstruiert und dabei lineare Codes verwendet. Digitale Netze werden bei quasi-Monte Carlo Methoden in der numerischen Integration benutzt.

J. Bierbrauer und der Autor haben die neuen Codes verwendet, um einige dichte Kugelpackungen in $\mathbb{R}^n$ zu konstruieren [6]. Desweiteren benötigen einige der klassischen Gitterkonstruktionen (siehe [12]), welche lineare Codes verwenden, nur deren Additivität. Hier kann man also die verallgemeinerten BCH-Codes verwenden.

Eine Anwendung, die essentiell die verallgemeinerten BCH-Codes benutzt, ist die Konstruktion einer Familie pseudogeometrischer, stark regulärer Graphen durch J. Bierbrauer und den Autor [7]. Dabei benutzt man eine Konstruktion stark regulären Graphen aus linearen Codes, welche nur zwei Gewichten besitzen (siehe z.B. [10]).

Da sich der hier gewählte Ansatz die BCH-Codes darzustellen und zu verallgemeinern als fruchtbar erwiesen hat, sollte man auch versuchen, ihn auf verwandte Klassen von Codes zu übertragen. Naheliegend wären zum Beispiel die “alternant Codes”, die die klassischen Goppa-Codes als Spezialfälle enthalten. Man erhält diese als Teilkörper-Teilcodes einer leichten Verallgemeinerung der Reed-Solomon-Codes (siehe z.B. [27, 24, 22]).

Am Ende angelangt, schließe ich somit in der Hoffnung, daß diese Arbeit den Ausgangspunkt für weitere Ergebnisse bildet.

A Codes aus Abschnitt 1.3

A.1 Codes aus Satz 1.23

$q = 2$

$\mathcal{E}$	$\mathcal{C}$	$\mathcal{D}$
$[211, 97, 32]$	$[206, 96, 31]$	$[3, 1, 3]$
$[133, 37, 34]$	$[126, 36, 34]$	$[6, 1, 6]$
$[136, 37, 36]$	$[127, 36, 35]$	$[7, 1, 7]$
$[139, 33, 38]$	$[132, 32, 37]$	$[5, 1, 5]$
$[133, 30, 40]$	$[123, 29, 39]$	$[8, 1, 8]$
$[137, 30, 42]$	$[126, 29, 42]$	$[10, 1, 10]$
$[202, 66, 42]$	$[197, 65, 41]$	$[3, 1, 3]$
$[147, 30, 46]$	$[135, 29, 45]$	$[10, 1, 10]$
$[152, 30, 48]$	$[140, 29, 48]$	$[11, 1, 11]$
$[219, 63, 48]$	$[215, 62, 47]$	$[2, 1, 2]$
$[158, 30, 49]$	$[148, 29, 49]$	$[9, 1, 9]$
$[205, 52, 50]$	$[200, 51, 50]$	$[4, 1, 4]$
$[210, 54, 50]$	$[199, 51, 49]$	$[7, 3, 4]$
$[164, 30, 52]$	$[153, 29, 52]$	$[10, 1, 10]$
$[209, 52, 52]$	$[203, 51, 51]$	$[4, 1, 4]$
$[212, 53, 52]$	$[203, 51, 51]$	$[6, 2, 4]$
$[203, 45, 54]$	$[197, 44, 54]$	$[5, 1, 5]$
$[207, 45, 56]$	$[200, 44, 56]$	$[6, 1, 6]$
$[220, 52, 56]$	$[214, 51, 55]$	$[4, 1, 4]$
$[204, 41, 58]$	$[196, 40, 57]$	$[6, 1, 6]$
$[214, 45, 58]$	$[208, 44, 57]$	$[4, 1, 4]$
$[219, 46, 58]$	$[215, 45, 58]$	$[3, 1, 3]$
$[208, 41, 60]$	$[199, 40, 59]$	$[7, 1, 7]$
$[218, 45, 60]$	$[211, 44, 59]$	$[5, 1, 5]$
$[215, 45, 58]$	$[209, 44, 58]$	$[5, 1, 5]$
$[216, 41, 62]$	$[209, 40, 62]$	$[6, 1, 6]$
$[233, 49, 62]$	$[228, 48, 61]$	$[3, 1, 3]$
$[241, 53, 62]$	$[236, 52, 61]$	$[3, 1, 3]$
$[217, 37, 66]$	$[208, 36, 65]$	$[7, 1, 7]$
$[257, 57, 66]$	$[252, 56, 65]$	$[3, 1, 3]$

$q = 3$

$\mathcal{E}$	$\mathcal{C}$	$\mathcal{D}$
$[43, 25, 9]$	$[40, 24, 9]$	$[2, 1, 2]$
$[46, 25, 10]$	$[43, 24, 10]$	$[2, 1, 2]$
$[114, 80, 12]$	$[112, 79, 12]$	$[1, 1, 1]$
$[62, 33, 13]$	$[59, 32, 13]$	$[2, 1, 2]$
$[114, 75, 14]$	$[112, 74, 14]$	$[1, 1, 1]$
$[97, 57, 15]$	$[95, 56, 15]$	$[1, 1, 1]$
$[114, 72, 15]$	$[112, 71, 15]$	$[1, 1, 1]$
$[67, 33, 16]$	$[62, 32, 16]$	$[4, 1, 4]$
$[70, 33, 18]$	$[64, 32, 18]$	$[5, 1, 5]$
$[114, 65, 18]$	$[112, 64, 18]$	$[1, 1, 1]$
$[64, 22, 20]$	$[60, 21, 20]$	$[3, 1, 3]$
$[122, 67, 20]$	$[120, 66, 20]$	$[1, 1, 1]$
$[56, 14, 22]$	$[52, 13, 22]$	$[3, 1, 3]$
$[114, 56, 22]$	$[112, 55, 22]$	$[1, 1, 1]$
$[56, 13, 23]$	$[51, 12, 23]$	$[4, 1, 4]$
$[129, 67, 23]$	$[127, 66, 23]$	$[1, 1, 1]$
$[67, 18, 24]$	$[64, 17, 24]$	$[2, 1, 2]$
$[68, 17, 25]$	$[65, 16, 25]$	$[2, 1, 2]$
$[72, 19, 25]$	$[70, 18, 25]$	$[1, 1, 1]$
$[115, 50, 26]$	$[112, 49, 26]$	$[2, 1, 2]$
$[120, 53, 26]$	$[118, 52, 26]$	$[1, 1, 1]$
$[114, 47, 27]$	$[111, 46, 27]$	$[2, 1, 2]$
$[115, 44, 29]$	$[113, 43, 29]$	$[1, 1, 1]$
$[77, 17, 31]$	$[71, 16, 31]$	$[5, 1, 5]$
$[86, 21, 31]$	$[83, 20, 31]$	$[2, 1, 2]$
$[115, 40, 32]$	$[112, 39, 32]$	$[2, 1, 2]$
$[80, 17, 33]$	$[73, 16, 33]$	$[6, 1, 6]$
$[114, 37, 33]$	$[111, 36, 33]$	$[2, 1, 2]$
$[119, 40, 33]$	$[117, 39, 33]$	$[1, 1, 1]$
$[83, 17, 35]$	$[75, 16, 35]$	$[7, 1, 7]$
$[92, 20, 35]$	$[89, 19, 35]$	$[2, 1, 2]$
$[114, 34, 35]$	$[111, 33, 35]$	$[2, 1, 2]$
$[119, 37, 35]$	$[117, 36, 35]$	$[1, 1, 1]$
$[94, 20, 36]$	$[90, 19, 36]$	$[3, 1, 3]$
$[86, 17, 37]$	$[77, 16, 37]$	$[8, 1, 8]$
$[96, 20, 37]$	$[93, 19, 37]$	$[2, 1, 2]$
$[119, 34, 37]$	$[117, 33, 37]$	$[1, 1, 1]$
$[115, 31, 38]$	$[112, 30, 38]$	$[2, 1, 2]$
$[89, 17, 39]$	$[79, 16, 39]$	$[9, 1, 9]$
$[122, 33, 39]$	$[120, 32, 39]$	$[1, 1, 1]$
$[115, 28, 40]$	$[112, 27, 40]$	$[2, 1, 2]$
$[92, 17, 41]$	$[81, 16, 41]$	$[10, 1, 10]$
$[112, 25, 41]$	$[109, 24, 41]$	$[2, 1, 2]$
$[125, 33, 41]$	$[122, 32, 41]$	$[2, 1, 2]$
$[115, 25, 42]$	$[112, 24, 42]$	$[2, 1, 2]$
$[120, 28, 42]$	$[118, 27, 42]$	$[1, 1, 1]$
$[113, 23, 43]$	$[110, 22, 43]$	$[2, 1, 2]$
$[119, 25, 44]$	$[117, 24, 44]$	$[1, 1, 1]$
$[100, 17, 45]$	$[90, 16, 45]$	$[9, 1, 9]$
$[116, 23, 45]$	$[112, 22, 45]$	$[3, 1, 3]$
$[121, 25, 45]$	$[118, 24, 45]$	$[2, 1, 2]$
$[114, 21, 46]$	$[110, 20, 46]$	$[3, 1, 3]$

$\mathcal{E}$	$\mathcal{C}$	$\mathcal{D}$
$[119, 23, 46]$	$[116, 22, 46]$	$[2, 1, 2]$
$[105, 17, 47]$	$[96, 16, 47]$	$[8, 1, 8]$
$[123, 24, 47]$	$[121, 23, 47]$	$[1, 1, 1]$
$[127, 26, 47]$	$[125, 25, 47]$	$[1, 1, 1]$
$[122, 23, 48]$	$[118, 22, 48]$	$[3, 1, 3]$
$[120, 21, 49]$	$[116, 20, 49]$	$[3, 1, 3]$
$[127, 23, 50]$	$[125, 22, 50]$	$[1, 1, 1]$
$[123, 21, 51]$	$[118, 20, 51]$	$[4, 1, 4]$
$[129, 23, 51]$	$[126, 22, 51]$	$[2, 1, 2]$
$[121, 19, 52]$	$[116, 18, 52]$	$[4, 1, 4]$
$[127, 21, 52]$	$[124, 20, 52]$	$[2, 1, 2]$
$[124, 19, 54]$	$[118, 18, 54]$	$[5, 1, 5]$
$[123, 17, 56]$	$[116, 16, 56]$	$[6, 1, 6]$
$[126, 17, 58]$	$[118, 16, 58]$	$[7, 1, 7]$
$[129, 17, 60]$	$[120, 16, 60]$	$[8, 1, 8]$
$[132, 17, 62]$	$[122, 16, 62]$	$[9, 1, 9]$

$q = 4$

$\mathcal{E}$	$\mathcal{C}$	$\mathcal{D}$
$[48, 23, 14]$	$[44, 22, 14]$	$[3, 1, 3]$
$[42, 15, 15]$	$[40, 14, 15]$	$[1, 1, 1]$
$[45, 15, 17]$	$[42, 14, 17]$	$[2, 1, 2]$
$[62, 28, 17]$	$[59, 27, 17]$	$[2, 1, 2]$
$[65, 28, 19]$	$[61, 27, 19]$	$[3, 1, 3]$
$[87, 43, 20]$	$[85, 42, 20]$	$[1, 1, 1]$
$[68, 28, 21]$	$[63, 27, 21]$	$[4, 1, 4]$
$[78, 34, 21]$	$[76, 33, 21]$	$[1, 1, 1]$
$[71, 28, 23]$	$[65, 27, 23]$	$[5, 1, 5]$
$[86, 37, 23]$	$[84, 36, 23]$	$[1, 1, 1]$
$[74, 28, 24]$	$[69, 27, 24]$	$[4, 1, 4]$
$[87, 33, 26]$	$[85, 32, 26]$	$[1, 1, 1]$
$[80, 28, 27]$	$[76, 27, 27]$	$[3, 1, 3]$
$[86, 31, 27]$	$[84, 30, 27]$	$[1, 1, 1]$
$[86, 28, 29]$	$[84, 27, 29]$	$[1, 1, 1]$
$[83, 23, 32]$	$[80, 22, 32]$	$[2, 1, 2]$
$[87, 24, 33]$	$[85, 23, 33]$	$[1, 1, 1]$
$[88, 23, 35]$	$[84, 22, 35]$	$[3, 1, 3]$
$[94, 25, 36]$	$[92, 24, 36]$	$[1, 1, 1]$
$[88, 20, 37]$	$[86, 19, 37]$	$[1, 1, 1]$
$[101, 27, 38]$	$[99, 26, 38]$	$[1, 1, 1]$
$[101, 25, 40]$	$[99, 24, 40]$	$[1, 1, 1]$
$[103, 24, 42]$	$[100, 23, 42]$	$[2, 1, 2]$
$[103, 23, 43]$	$[101, 22, 43]$	$[1, 1, 1]$
$[104, 22, 45]$	$[100, 21, 45]$	$[3, 1, 3]$
$[108, 24, 45]$	$[106, 23, 45]$	$[1, 1, 1]$
$[106, 22, 46]$	$[103, 21, 46]$	$[2, 1, 2]$
$[110, 24, 46]$	$[108, 23, 46]$	$[1, 1, 1]$
$[115, 27, 46]$	$[113, 26, 46]$	$[1, 1, 1]$
$[121, 30, 47]$	$[119, 29, 47]$	$[1, 1, 1]$
$[123, 30, 48]$	$[120, 29, 48]$	$[2, 1, 2]$
$[117, 24, 50]$	$[115, 23, 50]$	$[1, 1, 1]$
$[122, 26, 51]$	$[120, 25, 51]$	$[1, 1, 1]$
$[125, 26, 53]$	$[123, 25, 53]$	$[1, 1, 1]$
$[130, 28, 54]$	$[128, 27, 54]$	$[1, 1, 1]$

A.2 Codes aus Satz 1.24

$q = 3$

C_k	$\mathcal{C}_1$	$\iota(2), \ldots, \iota(k)$
$[118, 80, 13]$	$[111, 74, 13]$	1, 0, 0, 0, 0, 0
$[127, 88, 13]$	$[111, 74, 13]$	1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0
$[118, 75, 15]$	$[112, 71, 15]$	1, 1, 0, 0
$[125, 81, 15]$	$[112, 71, 15]$	1, 1, 0, 0, 1, 0, 0, 0, 0, 0
$[72, 35, 16]$	$[63, 32, 17]$	4, 1, 1
$[125, 79, 16]$	$[121, 76, 16]$	1, 0, 0
$[131, 84, 16]$	$[121, 76, 16]$	1, 0, 0, 1, 0, 0, 0, 0
$[132, 80, 18]$	$[127, 76, 18]$	1, 0, 0, 0
$[68, 25, 19]$	$[60, 21, 20]$	2, 1, 1, 0
$[100, 50, 19]$	$[95, 46, 19]$	1, 0, 0, 0
$[112, 60, 19]$	$[107, 56, 19]$	1, 0, 0, 0
$[130, 69, 22]$	$[126, 66, 22]$	1, 0, 0
$[115, 51, 25]$	$[111, 49, 25]$	2, 0
$[118, 53, 25]$	$[114, 50, 25]$	1, 0, 0
$[122, 56, 25]$	$[117, 52, 25]$	1, 0, 0, 0
$[124, 56, 26]$	$[112, 49, 26]$	2, 1, 1, 0, 1, 0, 0
$[120, 51, 27]$	$[117, 49, 27]$	1, 0
$[124, 54, 27]$	$[117, 49, 27]$	1, 0, 1, 0, 0
$[128, 57, 27]$	$[117, 49, 27]$	1, 0, 1, 0, 0, 1, 0, 0
$[121, 50, 28]$	$[112, 46, 28]$	3, 1, 1, 0
$[121, 48, 29]$	$[118, 46, 29]$	1, 0
$[125, 51, 29]$	$[118, 46, 29]$	1, 0, 1, 0, 0
$[120, 44, 31]$	$[117, 42, 31]$	1, 0
$[123, 46, 31]$	$[117, 42, 31]$	1, 0, 1, 0
$[122, 42, 33]$	$[117, 39, 33]$	1, 1, 0
$[94, 21, 35]$	$[75, 16, 35]$	7, 3, 2, 1, 1
$[96, 22, 35]$	$[75, 16, 35]$	7, 3, 2, 1, 1, 1
$[122, 39, 35]$	$[117, 36, 35]$	1, 1, 0
$[125, 41, 35]$	$[117, 36, 35]$	1, 1, 0, 1, 0
$[98, 21, 37]$	$[79, 16, 39]$	7, 3, 2, 1, 1
$[100, 22, 37]$	$[79, 16, 39]$	7, 3, 2, 1, 1, 1
$[122, 36, 37]$	$[117, 33, 37]$	1, 1, 0
$[125, 38, 37]$	$[117, 33, 37]$	1, 1, 0, 1, 0
$[128, 40, 37]$	$[124, 37, 37]$	1, 0, 0
$[125, 35, 39]$	$[120, 32, 39]$	1, 1, 0
$[129, 35, 41]$	$[126, 33, 41]$	1, 0
$[122, 29, 42]$	$[118, 27, 42]$	1, 1
$[125, 31, 42]$	$[118, 27, 42]$	1, 1, 1, 0
$[115, 24, 43]$	$[110, 22, 43]$	2, 1
$[117, 25, 43]$	$[110, 22, 43]$	2, 1, 1
$[119, 26, 43]$	$[110, 22, 43]$	2, 1, 1, 1
$[124, 29, 43]$	$[121, 27, 43]$	1, 0
$[127, 31, 43]$	$[121, 27, 43]$	1, 0, 1, 0
$[130, 33, 43]$	$[121, 27, 43]$	1, 0, 1, 0, 1, 0

C_k	$\mathcal{C}_1$	$\iota(2), \ldots, \iota(k)$
$[121, 26, 44]$	$[117, 24, 44]$	1, 1
$[126, 29, 44]$	$[123, 27, 44]$	1, 0
$[129, 31, 44]$	$[123, 27, 44]$	1, 0, 1, 0
$[128, 29, 45]$	$[125, 27, 45]$	1, 0
$[123, 25, 46]$	$[116, 22, 46]$	2, 1, 1
$[125, 26, 46]$	$[122, 24, 46]$	1, 0
$[130, 29, 46]$	$[127, 27, 46]$	1, 0
$[123, 22, 49]$	$[118, 20, 51]$	2, 1
$[125, 23, 49]$	$[118, 20, 51]$	2, 1, 1
$[127, 24, 49]$	$[118, 20, 51]$	2, 1, 1, 1
$[129, 25, 49]$	$[118, 20, 51]$	2, 1, 1, 1, 1
$[129, 24, 50]$	$[125, 22, 50]$	1, 1
$[129, 22, 52]$	$[124, 20, 52]$	2, 1
$[131, 23, 52]$	$[124, 20, 52]$	2, 1, 1

$q = 4$

C_k	$\mathcal{C}_1$	$\iota(2), \ldots, \iota(k)$
$[140, 129, 5]$	$[126, 116, 5]$	1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
$[75, 60, 7]$	$[70, 57, 7]$	2, 0, 0
$[111, 92, 8]$	$[108, 90, 8]$	1, 0
$[119, 99, 8]$	$[108, 90, 8]$	1, 0, 1, 0, 0, 0, 0, 0, 0
$[43, 26, 9]$	$[39, 24, 9]$	2, 0
$[95, 73, 9]$	$[85, 64, 9]$	1, 0, 0, 0, 0, 0, 0, 0, 0
$[112, 89, 9]$	$[85, 64, 9]$	1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
$[94, 70, 10]$	$[90, 67, 10]$	1, 0, 0
$[76, 51, 11]$	$[72, 48, 11]$	1, 0, 0
$[97, 70, 11]$	$[89, 63, 11]$	1, 0, 0, 0, 0, 0, 0
$[109, 81, 11]$	$[89, 63, 11]$	1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
$[88, 60, 12]$	$[85, 58, 12]$	1, 0
$[125, 94, 12]$	$[120, 90, 12]$	1, 0, 0, 0
$[49, 24, 13]$	$[44, 22, 14]$	2, 1
$[79, 49, 13]$	$[73, 44, 13]$	1, 0, 0, 0, 0
$[74, 43, 14]$	$[71, 41, 14]$	1, 0
$[79, 47, 14]$	$[71, 41, 14]$	1, 0, 1, 0, 0, 0
$[96, 62, 14]$	$[86, 53, 14]$	1, 0, 0, 0, 0, 0, 0, 0, 0
$[107, 72, 14]$	$[86, 53, 14]$	1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0
$[73, 40, 15]$	$[70, 38, 15]$	1, 0
$[86, 51, 15]$	$[79, 45, 15]$	1, 0, 0, 0, 0, 0
$[89, 52, 16]$	$[85, 49, 16]$	1, 0, 0
$[104, 65, 16]$	$[96, 58, 16]$	1, 0, 0, 0, 0, 0, 0
$[65, 30, 17]$	$[59, 27, 17]$	2, 1, 0
$[69, 33, 17]$	$[59, 27, 17]$	2, 1, 0, 1, 0, 0
$[74, 37, 17]$	$[59, 27, 17]$	2, 1, 0, 1, 0, 0, 1, 0, 0, 0
$[80, 42, 17]$	$[59, 27, 17]$	2, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0
$[67, 30, 18]$	$[61, 27, 19]$	2, 1, 0
$[71, 33, 18]$	$[60, 27, 18]$	3, 1, 0, 1, 0, 0
$[81, 41, 18]$	$[75, 36, 18]$	1, 0, 0, 0, 0
$[111, 67, 18]$	$[102, 59, 18]$	1, 0, 0, 0, 0, 0, 0, 0

C_k	$\mathcal{C}_1$	$\iota(2), \ldots, \iota(k)$
$[70, 31, 19]$	$[61, 27, 19]$	3, 1, 1, 0
$[89, 46, 19]$	$[84, 42, 19]$	1, 0, 0, 0
$[91, 46, 20]$	$[85, 42, 20]$	1, 1, 0, 0
$[86, 40, 21]$	$[81, 36, 21]$	1, 0, 0, 0
$[119, 68, 21]$	$[111, 61, 21]$	1, 0, 0, 0, 0, 0, 0
$[88, 40, 22]$	$[85, 38, 22]$	1, 0
$[93, 44, 22]$	$[87, 39, 22]$	1, 0, 0, 0, 0
$[99, 49, 22]$	$[87, 39, 22]$	1, 0, 0, 0, 0, 1, 0, 0, 0, 0
$[90, 40, 23]$	$[84, 36, 23]$	1, 1, 0, 0
$[95, 44, 23]$	$[84, 36, 23]$	1, 1, 0, 0, 1, 0, 0, 0
$[120, 65, 23]$	$[113, 59, 23]$	1, 0, 0, 0, 0, 0
$[89, 38, 24]$	$[85, 36, 24]$	2, 0
$[92, 40, 24]$	$[85, 36, 24]$	2, 0, 1, 0
$[97, 44, 24]$	$[85, 36, 24]$	2, 0, 1, 0, 1, 0, 0, 0
$[108, 53, 24]$	$[102, 48, 24]$	1, 0, 0, 0, 0
$[121, 64, 24]$	$[114, 58, 24]$	1, 0, 0, 0, 0, 0
$[82, 31, 25]$	$[72, 27, 25]$	4, 1, 1, 0
$[85, 33, 25]$	$[72, 27, 25]$	4, 1, 1, 0, 1, 0
$[89, 36, 25]$	$[72, 27, 25]$	4, 1, 1, 0, 1, 0, 1, 0, 0
$[122, 63, 25]$	$[115, 57, 25]$	1, 0, 0, 0, 0, 0
$[81, 29, 26]$	$[76, 27, 27]$	2, 1
$[91, 36, 26]$	$[85, 32, 26]$	1, 1, 0, 0
$[117, 57, 26]$	$[111, 52, 26]$	1, 0, 0, 0, 0
$[89, 33, 27]$	$[85, 30, 28]$	1, 0, 0
$[93, 36, 27]$	$[88, 32, 27]$	1, 0, 0, 0
$[91, 33, 28]$	$[85, 30, 28]$	2, 1, 0
$[126, 61, 28]$	$[120, 56, 28]$	1, 0, 0, 0, 0
$[96, 34, 30]$	$[82, 25, 30]$	2, 1, 0, 1, 0, 0, 1, 0, 0
$[100, 37, 30]$	$[82, 25, 30]$	2, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0
$[104, 40, 30]$	$[99, 36, 30]$	1, 0, 0, 0
$[91, 29, 31]$	$[87, 27, 31]$	2, 0
$[98, 34, 31]$	$[94, 31, 31]$	1, 0, 0
$[102, 37, 31]$	$[94, 31, 31]$	1, 0, 0, 1, 0, 0
$[90, 27, 32]$	$[87, 25, 32]$	1, 0
$[93, 29, 32]$	$[89, 26, 32]$	1, 0, 0
$[89, 25, 33]$	$[85, 23, 33]$	1, 1
$[92, 27, 33]$	$[85, 23, 33]$	1, 1, 1, 0
$[99, 32, 33]$	$[95, 29, 33]$	1, 0, 0
$[109, 38, 34]$	$[105, 35, 34]$	1, 0, 0
$[113, 41, 34]$	$[108, 37, 34]$	1, 0, 0, 0
$[92, 25, 35]$	$[84, 22, 35]$	3, 1, 1
$[94, 26, 35]$	$[91, 24, 35]$	1, 0
$[97, 28, 35]$	$[91, 24, 35]$	1, 0, 1, 0
$[124, 48, 35]$	$[119, 44, 35]$	1, 0, 0, 0
$[103, 31, 36]$	$[100, 29, 36]$	1, 0

C_k	$\mathcal{C}_1$	$\iota(2), \ldots, \iota(k)$
$[110, 36, 36]$	$[106, 33, 36]$	1, 0, 0
$[116, 39, 37]$	$[112, 36, 37]$	1, 0, 0
$[120, 42, 37]$	$[112, 36, 37]$	1, 0, 0, 1, 0, 0
$[111, 34, 38]$	$[107, 31, 38]$	1, 0, 0
$[104, 28, 39]$	$[100, 26, 39]$	2, 0
$[107, 30, 39]$	$[100, 26, 39]$	2, 0, 1, 0
$[110, 32, 39]$	$[106, 29, 39]$	1, 0, 0
$[117, 37, 39]$	$[113, 34, 39]$	1, 0, 0
$[121, 40, 39]$	$[113, 34, 39]$	1, 0, 0, 1, 0, 0
$[103, 26, 40]$	$[99, 24, 40]$	1, 1
$[106, 28, 40]$	$[99, 24, 40]$	1, 1, 1, 0
$[116, 35, 40]$	$[112, 32, 40]$	1, 0, 0
$[127, 43, 40]$	$[123, 40, 40]$	1, 0, 0
$[122, 38, 41]$	$[118, 35, 41]$	1, 0, 0
$[105, 25, 42]$	$[101, 22, 43]$	0, 1, 0
$[108, 27, 42]$	$[101, 22, 43]$	0, 1, 0, 1, 0
$[111, 29, 42]$	$[101, 22, 43]$	0, 1, 0, 1, 0, 1, 0
$[128, 41, 42]$	$[124, 38, 42]$	1, 0, 0
$[105, 24, 43]$	$[101, 22, 43]$	1, 1
$[113, 28, 44]$	$[110, 26, 44]$	1, 0
$[116, 30, 44]$	$[110, 26, 44]$	1, 0, 1, 0
$[110, 25, 45]$	$[106, 23, 45]$	1, 1
$[121, 31, 46]$	$[118, 29, 46]$	1, 0
$[124, 33, 46]$	$[120, 30, 46]$	1, 0, 0
$[126, 32, 48]$	$[120, 29, 48]$	2, 1, 0
$[129, 34, 48]$	$[120, 29, 48]$	2, 1, 0, 1, 0
$[117, 25, 49]$	$[114, 23, 49]$	1, 0
$[125, 29, 50]$	$[122, 27, 50]$	1, 0
$[128, 31, 50]$	$[122, 27, 50]$	1, 0, 1, 0
$[130, 30, 52]$	$[127, 28, 52]$	1, 0

A.3 Codes aus Satz 1.24 mit Konstruktion X

$q = 2$

$\mathcal{E}$	$\mathcal{C}_k$	$\mathcal{C}_1$	$\mathcal{D}$	$\iota(2), \ldots, \iota(k)$
$[153, 31, 46]$	$[137, 31, 35]$	$[135, 29, 45]$	$[15, 2, 10]$	0, 0
$[158, 31, 48]$	$[142, 31, 37]$	$[140, 29, 48]$	$[15, 2, 10]$	0, 0
$[208, 57, 48]$	$[204, 57, 45]$	$[200, 55, 48]$	$[3, 2, 2]$	1, 1
$[208, 53, 50]$	$[202, 53, 46]$	$[200, 51, 50]$	$[6, 2, 4]$	0, 0
$[210, 52, 52]$	$[206, 52, 48]$	$[204, 51, 52]$	$[4, 1, 4]$	1

$q = 3$

$\mathcal{E}$	$\mathcal{C}_k$	$\mathcal{C}_1$	$\mathcal{D}$	$\iota(2), \ldots, \iota(k)$
$[68, 34, 15]$	$[64, 34, 12]$	$[62, 32, 16]$	$[4, 2, 3]$	0, 0
$[70, 34, 16]$	$[66, 34, 13]$	$[63, 32, 17]$	$[4, 2, 3]$	1, 0
$[73, 34, 18]$	$[69, 34, 15]$	$[64, 32, 18]$	$[4, 2, 3]$	2, 1
$[66, 23, 20]$	$[62, 23, 17]$	$[60, 21, 20]$	$[4, 2, 3]$	0, 0
$[57, 15, 21]$	$[53, 15, 18]$	$[51, 13, 21]$	$[4, 2, 3]$	0, 0
$[58, 13, 24]$	$[54, 13, 20]$	$[52, 12, 24]$	$[4, 1, 4]$	1
$[115, 53, 24]$	$[114, 53, 23]$	$[112, 52, 24]$	$[1, 1, 1]$	1
$[116, 47, 28]$	$[114, 47, 26]$	$[112, 46, 28]$	$[2, 1, 2]$	1
$[118, 48, 28]$	$[115, 48, 26]$	$[112, 46, 28]$	$[3, 2, 2]$	1, 0
$[117, 44, 30]$	$[114, 44, 28]$	$[112, 42, 30]$	$[3, 2, 2]$	0, 0
$[86, 19, 33]$	$[77, 19, 27]$	$[73, 16, 33]$	$[9, 3, 6]$	0, 0, 1
$[88, 20, 33]$	$[78, 20, 27]$	$[73, 16, 33]$	$[10, 4, 6]$	0, 0, 1, 0
$[121, 40, 34]$	$[120, 40, 33]$	$[118, 39, 34]$	$[1, 1, 1]$	1
$[87, 18, 35]$	$[79, 18, 29]$	$[77, 16, 37]$	$[8, 2, 6]$	0, 0
$[121, 37, 36]$	$[120, 37, 35]$	$[118, 36, 36]$	$[1, 1, 1]$	1
$[90, 18, 37]$	$[79, 18, 29]$	$[77, 16, 37]$	$[11, 2, 8]$	0, 0
$[94, 19, 38]$	$[81, 19, 29]$	$[78, 16, 38]$	$[13, 3, 9]$	0, 0, 0
$[121, 34, 38]$	$[120, 34, 37]$	$[118, 33, 38]$	$[1, 1, 1]$	1
$[93, 18, 39]$	$[81, 18, 30]$	$[79, 16, 39]$	$[12, 2, 9]$	0, 0
$[96, 19, 39]$	$[83, 19, 30]$	$[79, 16, 39]$	$[13, 3, 9]$	0, 0, 1
$[99, 20, 39]$	$[84, 20, 30]$	$[79, 16, 39]$	$[15, 4, 9]$	0, 0, 1, 0
$[95, 18, 40]$	$[83, 18, 31]$	$[81, 16, 41]$	$[12, 2, 9]$	0, 0
$[98, 19, 40]$	$[85, 19, 31]$	$[81, 16, 41]$	$[13, 3, 9]$	0, 0, 1
$[101, 20, 40]$	$[86, 20, 31]$	$[81, 16, 41]$	$[15, 4, 9]$	0, 0, 1, 0
$[97, 18, 41]$	$[85, 18, 32]$	$[82, 16, 42]$	$[12, 2, 9]$	1, 0
$[100, 19, 41]$	$[87, 19, 32]$	$[82, 16, 42]$	$[13, 3, 9]$	1, 0, 1
$[115, 26, 41]$	$[114, 26, 40]$	$[112, 25, 41]$	$[1, 1, 1]$	1
$[127, 34, 41]$	$[124, 34, 39]$	$[122, 32, 41]$	$[3, 2, 2]$	0, 0
$[94, 17, 42]$	$[84, 17, 32]$	$[82, 16, 42]$	$[10, 1, 10]$	1
$[99, 18, 42]$	$[84, 18, 31]$	$[82, 16, 42]$	$[15, 2, 11]$	0, 0
$[102, 19, 42]$	$[85, 19, 31]$	$[82, 16, 42]$	$[17, 3, 11]$	0, 0, 0
$[101, 18, 43]$	$[89, 18, 34]$	$[87, 16, 43]$	$[12, 2, 9]$	0, 0
$[104, 19, 43]$	$[91, 19, 34]$	$[88, 16, 44]$	$[13, 3, 9]$	0, 0, 0
$[123, 26, 45]$	$[120, 26, 43]$	$[118, 24, 45]$	$[3, 2, 2]$	0, 0
$[121, 24, 46]$	$[118, 24, 44]$	$[116, 22, 46]$	$[3, 2, 2]$	0, 0
$[124, 24, 48]$	$[120, 24, 45]$	$[118, 22, 48]$	$[4, 2, 3]$	0, 0
$[129, 26, 48]$	$[128, 26, 47]$	$[126, 25, 48]$	$[1, 1, 1]$	1
$[132, 22, 54]$	$[128, 22, 51]$	$[126, 20, 54]$	$[4, 2, 3]$	0, 0
$[130, 18, 58]$	$[122, 18, 52]$	$[118, 16, 58]$	$[8, 2, 6]$	1, 1

$q = 4$

$\mathcal{E}$	$\mathcal{C}_k$	$\mathcal{C}_1$	$\mathcal{D}$	$\iota(2), \ldots, \iota(k)$
$[67, 29, 19]$	$[63, 29, 16]$	$[61, 27, 19]$	$[4, 2, 3]$	0, 0
$[70, 29, 21]$	$[65, 29, 17]$	$[63, 27, 21]$	$[5, 2, 4]$	0, 0
$[73, 29, 23]$	$[68, 29, 19]$	$[65, 27, 23]$	$[5, 2, 4]$	1, 0
$[76, 29, 24]$	$[71, 29, 20]$	$[69, 27, 24]$	$[5, 2, 4]$	0, 0
$[77, 28, 25]$	$[74, 28, 22]$	$[72, 27, 25]$	$[3, 1, 3]$	1
$[79, 29, 25]$	$[75, 29, 22]$	$[72, 27, 25]$	$[4, 2, 3]$	1, 0
$[88, 31, 28]$	$[87, 31, 27]$	$[85, 30, 28]$	$[1, 1, 1]$	1
$[90, 24, 35]$	$[86, 24, 32]$	$[84, 22, 35]$	$[4, 2, 3]$	0, 0
$[90, 23, 36]$	$[87, 23, 33]$	$[85, 22, 36]$	$[3, 1, 3]$	1

B Erzeuger- und Checkmatrizen

Erzeugermatrix eines binären $[38, 12, 13]$.

$$
\begin{array}{l}
10000000000011100010100011100111111010 \\
01000000000010111011110010010100011000 \\
00100000000000101111010010101011110101 \\
00010000000001010000010111000100111011 \\
00001000000011011110101100000110001000 \\
00000100000001100101111101100010100111 \\
00000010000011100110110010110100100101 \\
00000001000010000010000110011010111101 \\
00000000100010111101001111001000001001 \\
00000000010011111011010101111111100001 \\
00000000001000110110111111011111101110 \\
00000000000101111010101011100001001101
\end{array}
$$

Checkmatrix eines binären $[71, 46, 9]$.

$$
\begin{array}{l}
10000000000000000000000001001100110101110101010101000110110110011000000 \\
01000000000000000000000001111011111011111001000000011110001101010010110 \\
00100000000000000000000001000101010011011011111111101110000000101011110 \\
00010000000000000000000001000101010011011011111111101110000000100111100 \\
00001000000000000000000001011111111000101000000000010111011011111011001 \\
00000100000000000000000001101010101111001111111111100101101101010110101 \\
00000010000000000000000001010111010010110011011111101010101011111101101 \\
00000001000000000000000001000001000110010110010000010000111000101001001 \\
00000000100000000000000001111010111110101010011011100001100011010110010 \\
00000000010000000000000001000001000110010110010000010000111000011000011 \\
00000000001000000000000001010111110000011010110010010101011100111000100 \\
00000000000100000000000001000001010111000010100110101111000011000101011 \\
00000000000010000000000001000001010111000010100110101111000011000011101 \\
00000000000001000000000001000001010111000010100110101111000011101000000 \\
00000000000000100000000001100010100101110111110101101000001010100110011 \\
00000000000000010000000001100010100101110111110101101000001010100110000 \\
00000000000000001000000001100010100101110111110101101000001010110000001 \\
00000000000000000100000011001101110111000010000101111111011111110010010 \\
00000000000000000010000001011001110010111111011110111010011010101001000 \\
00000000000000000001000000101100111001011111101111011101001101011011100 \\
00000000000000000000100001111111100010100000000001011101101111011000010 \\
00000000000000000000010001010100110110111111111011100000001000101101101 \\
00000000000000000000001000101010011011011111111101110000000100011011101 \\
00000000000000000000000101111100110011100000001000001011001011111101001 \\
00000000000000000000000011010101011110011111111111001011011010110110000
\end{array}
$$

Checkmatrix eines binären $[161, 138, 7]$.
Die Checkmatrix eines binären $[154, 132, 7]$ erhält man durch Einschränkung auf die ersten 154 Spalten und 22 Zeilen.

```
01111111111111111111111111111111111111111111111111111111111111111111111111111111
00000001000001100001010001111001000101100111010100111110100001110001001001101101
00000010000011000010100011110010001011001110101001111101000011100010010011011010
00000100000110000101000111100100010110011101010011111010000111000100100110110101
00001000001100001010001111001000101100111010100111110100001110001001001101101011
00010000011000010100011110010001011001110101001111101000011100010010011011010110
00100000110000101000111100100010110011101010011111010000111000100100110110101101
01000001100001010001111001000101100111010100111110100001110001001001101101011011
00000001010000110110010000011110001011010110000100010011101111010001100110100110
00101010111010100100101111111001111101101110000001010000110110010000011110001011
00001000100111011110100011001101001100011100101010111010100100101111111001111011
00000010100001101100100000111100010110101100001000100111011110100011001101001100
01010101110101001001011111110011111011011100000010100001101100100000111100010110
00010001001110111101000110011010011000111001010101110101001001011111110011111011
00000101000011011001000001111000101101011000010001001110111101000110011010011000
01010101110101001001011111110011111011011100000010100001101100100000111100010110
00010001001110111101000110011010011000111001010101110101001001011111110011111011
00000101000011011001000001111000101101011000010001001110111101000110011010011000
00001110101110011100011011001100000010001111101001101000101111011011011111110000
01000101111011011101111111000010101100010011110010100100101101010100000110010001
00100101101010100000110010000111010111001110001101100110000001000111101001101000
00110000001000111110100110100010111101101110111111100001010110001001111001010010
00001010110001001111001010010010110101010000011001000011101011100111000110110011
00011101011100111000110110011000000100011111010011010001011110110111011111100001
00000000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
11111111111111111111111111111111111111111111111100000000000000000000000000000000
11011110110001101001011101110011001010101111111000000000000000000000000000000000
10111101100011010010111011100110010101011111110000000000000000000000000000000000
01111011000110100101110111001100101010111111100000000000000000000000000000000000
11110110001101001011101110011001010101111111000000000000000000000000000000000000
11101100011010010111011100110010101011111110000000000000000000000000000000000000
11011000110100101110111001100101010111111100000000000000000000000000000000000000
10110001101001011101110011001010101111111000000000000000000000000000000000000000
01110010101011101010010010111111100111110110111100000100001000101011110100011110
10110000100010011101111010001100110100110001110010000100111000011110101000100100
01110000001010000110110010000011110001011010110001000100010001001010110110111110
11100101010111010100100101111111001111101101110000010010100100011001100010010000
01100001000100111011110100011001101001100011100000010100010111011000111110010000
11100000010100001101100100000111100010110101100000001100010101101101000110100111
11001010101110101001001011111110011111011011100000000010010110100101111100111000
00000010001111101001101000101111011011101111111000000001010100101100001110101100
10101100010011110010100100101101010100000110010000000000110010001000111000011001
11010111001110001101100110000001000111110100110000000000001110000101000010000110
10111101101110111111100001010110001001111001010000000000000011001001010100011110
10110101010000011001000011101011100111000110110000000000000000011100001010000101
00000100011111010011010001011110110111011111110000000000000000000011100110000101
01011000100111100101001001011010101000001100100000000000000000000011110000011
00000000000000000000000000000000000000000000000000000000000000000000000001111111
```

Checkmatrix eines ternären $[86, 77, 5]$
= Erzeugermatrix eines ternären $[86, 9, 50]$

```
10000000020220211012220012210211000212201101110110121220020001121202021211000200211112
01000000011011001020220220201020212112101020212101020201012120220201012101012120222000
00100000010101100022202220122121001112100202202112100202001211100121220001211202100 21
00010000000000000000000000001111111111111111111111111122222222222222222222222222200000
00001000001100022200011122202110221010210210202121010201220112012020101201201201222202
00000100010221102000201102020201102022120021211012210111012210122120021200201102001222
00000010011002211202200112110101010012110022021122001011212121101002211221122001001200
00000001000001122222211100001220112001201201220101212002110221002121010221021021011101
00000000120212001122121220020221212222110101100221212222102012200210120000210120021111
```

Checkmatrix eines ternären $[134, 123, 5]$

```
11111111111111111111111111111111111111111111111111111111111111111111111
02010121210021222201022021110000102001112112122022100011220122002 00
00010002112020021021202101100202022020120022011210222221122210202 1
00101212100212222010220211100001020011121121220221000112201220020 00
00100021120200210212021011002020222020120022011210222221122210202 12
01012121002122220102202111000010200111211212202210001122012200200 01
02111101221201100001112202001212000211021110200010010121011211002 20
00102100201011022222102011222121222020211210220000222110100212100 012
00022022200221001201211221012020201200102022011111201022111212111 10
00001220122201000200202120221220011011100112002102122112021010102 10
01111012212011000011122020012120002110211102000100101210112110022 02
```

```
11111111111111111111111111111111111111111111111111111111212211221221
01221010012012101202200101011101021001102212011111221110000000000000
21200121111020110122200002010022212212110112000221102110000000000000
12210100120121012202001010111010210011022120111112211120000000000000
12001211110201101222000020100222122121101120002211021100000000000000
22101001201210120220010101110102100110221201111122111200000000000000
22200221001201211221012020201200102022011111201022111211002012001 12
20122201000200202120221220011011100112002102122112021010101002012 11
12212011000011122020012120002110211102000100101210112110011012011 01
02010110222221020112221212222021121022000022211010021210000111000 11
22002210012012112210120202012001020220111112010221112120000000111 11
```

Checkmatrix eines ternären $[116, 102, 6]$
Die Checkmatrix eines ternären $[103, 90, 6]$, $[95, 83, 6]$ bzw. $[85, 74, 6]$ erhält man durch Einschränkung auf die ersten 103, 95 bzw. 85 Spalten und 13, 12 bzw. 11 Zeilen.

```
10000000000110002001002112122012111101112022112020102221102101002111202111020122
01000000000121102100120102110210200112110100012210001021221221000212002102201210
00100000000012022101000221101121020011210020102221000102221221100020210210220121
00010000000200011122012222002211101012000200210212211000120201101001021100112220
00001000000210211211100122111220021211100202011221120202122211011101002020101001
00000100000000211121002001212012101001122022000222200012011221120002101021022012
00000010000101122102201110022202112121112010110110212000021010021000022002020011
00000001000112221022012121121020111200111022122102110200210220201202011100120111
00000000100011211210212101112210012120012122021210111022001210010220011110012011
00000000010101101110101222122200201200002020211212100100121200200022110011222011
00000000001012002201122021220221020120002201002121110011001021010001111001122201
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
12110022212122002112120021220101112 1
01210001220121002101102010010021201 2
02211000111102200212120012111211002 0
10210010011000201220012001111000121 2
12102012022120101111121002011220202 0
12112010002210000200101010012102012 2
10012001021211000210200000000201020 2
00121000100201000000001001010200001 2
11020000021020200110001001000100000 1
02121000000110100110002001000000000 0
10220000001112200010000000000000000 0
00000111111111100001122000112200112 2
00000000000000011111111000000011111 1
00000000000000000000000011111111111 1
```

Checkmatrix eines ternären q=3 $[52, 38, 7]$
Die Checkmatrix eines ternären $[42, 29, 7]$ bzw. $[33, 21, 7]$ erhält man durch Einschränkung auf die ersten 42 bzw. 33 Spalten und 13 bzw. 12 Zeilen.

```
0202122102220010121120111000000020202122000100010212
2021221022200101211201110000010010111012210221121102
0212210222001012112011100200020020011021210002202110
2221220021010222122002101002002100120100110100210121
0120201112110012020111211021202100001112010011222010
2212200210102221220021010201101200000021010012211012
2120112220200212011222020010200000000002210000020012
1001210221110100121022111001001200000000120000112000
2202002120112220200212011200100000000002020000121010
1211120011010212221002202000012210000022210000002001
2202012111200110102122210000001120000000020000000012
2210022020121112001101021200001110000001220000000002
0000000000000000000000000000000001111111110000000112
0000000000000000000000000000000000000000001111111111
```

Checkmatrix eines ternären $[34, 20, 8]$

```
1000000000000200222202110000120112
0100000000000022121212200110201101
0010000000000010112000102210212022
0001000000000101111221012010112222
0000100000000021101021211110112010
0000010000000121121111222210021010
0000001000000202100010210110100221
0000000100000000000111111110011222
0000000010000110000210212100001012
0000000001000202001120220020001120
0000000000100000110211021020000121
0000000000010112211210010110000020
0000000000001012200101102010000002
0000000000000000000000000001111111
```

Checkmatrix eines ternären $[44, 29, 8]$

$$
\begin{array}{l}
10000000000000012002102222221212022121002110\\
01000000000000012212111200002000202200122112\\
00100000000000012020100120002021110102211222\\
00010000000000011102222000002121120212202212\\
00001000000000020100121012001111021101022202\\
00000100000000010112201101202202222022001212\\
00000010000000021222011111010022120020101120\\
00000001000000020212001110121102102020001112\\
00000000100000021020012111102211122120111011\\
00000000010000021000112211111100022000112100\\
00000000001000010202200221110201122112210200\\
00000000000100022000100002212011221012220011\\
00000000000010001020220022111020112211221201\\
00000000000001002200010000221201122101222201\\
00000000000000011102222000002121120212202100 1
\end{array}
$$

Erzeugermatrix eines ternären $[25, 10, 10]$

$$
\begin{array}{l}
11121010012002210000000 0\\
21200011112101101000000 00\\
12002120101110200100000 00\\
21021022220010200010000 00\\
01220211200202200001000 00\\
11210100102022100000100 00\\
20012210120200200000010 00\\
00222122111112000000001 00\\
02212001022210000000000 10\\
21022220010021000000000 01
\end{array}
$$

Checkmatrix eines ternären $[108, 91, 7]$
Die Checkmatrix eines ternären $[92, 76, 7]$ erhält man durch Einschränkung auf die ersten 92 Spalten und 16 Zeilen.

```
000000000000001212020111202111100122001122120010112201
000000000000010110221220022222101012012011121111201212
000000000000100112222121000101210001122002021102200221
000000000001000012201102201012000222222101020012220010
000000000010000221011021020201002222221120000122200100
000000001000000111000211012111220112121212202021102000
000000010000001110002112101112201121211222020211020000
000000100000002220120022220101010022101102022012111101
000001000000001111110100221122110111102120012022220210
000010000000000202111220220101001022020220200212120202
000010000000000122102011021211110012200121022101011220
000100000000000011120212212021121011222212202120221201
001000000000000220002122011221220212122111202200112122
010000000000000212001110200110001000221001101012011201
100000000000000222101211012221120221111102211101121020
000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000

111110112202212011120002201100202002210001101020020010
122221100120100112022022201210101002210201200122222100
010122102111120000112220102021201201200102111212122220
102222002010221122000210112102001100020122022102222211
221202100222012012020011120210001121100111210022200222
000210000200101012021010101121200110100112202011002012
020001020010012001200111010112200112000010010101202012
022210021102112222221002222211000010110011120022001211
101001122010101200022122111021200012020002220120101120
020010022011101012122210212002000001120002200000212011
111101212112021112010220021000200000200002010000001221
201210001122022110110111022120100002010000220000100120
212020012102101012102222222011200001220000000000110202
002100200120022100011121122221200000120000000000010011
011202120201110222222002100121200001110000000000020012
000000000000000000000000000000000011111110000001112112222
000000000000000000000000000000000000001111111111111111
```

Checkmatrix eines quaternären $[145, 135, 5]$
Die Checkmatrix eines quaternären $[87, 78, 5]$ erhält man durch Einschränkung auf die ersten 87 Spalten und 9 Zeilen.

```
000000011030020201233131321303123311120021302020121100102311121130210133123333 02
000000102030221021102222213332231000320232322232130101121200330100112022121120 03
000001001012221200333030203223232012032311321323033211011211332101012302320121 0
000010000232230121103233001131100110203132111223213010013100213120011330013021 00
000100003222301112032330110311100021031321112221330100131002131020000001112001 33
001000001203002112201022222313302231003202323223212301011212003300000000000011121
010000001310002010223313113230333112112002130201202110010231112130000000000000001
100000001233121322332011322112011110302310112123110131223322221310000000000000000
000000000000000000000000000000000000000000000000000000000000000000000111111111111111
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
013013103223013100123203212232233003331221130010102312332021231 33
232321101033122123111331023303231210202231003130321301123132031 32
003221001213311200002323333213001211133212113202200011102020220 33
212211100123023003131202013201000223012321202120023000120202002 01
323102000000112012031100231121301130123213230020312123210202111 02
111302200000000111220011032001122230002033211302212112200330221 32
310030300000000000001112102000000001111230130011122301022132330 13
012223300000000000000001220000000000000011300000000112230011233 3
111111100000000000000000011111111111111111122222222222233333333
000000011111111111111111111111111111111111111111111111111111111
```

Checkmatrix eines quaternären $[106, 94, 6]$
Die Checkmatrix eines quaternären $[81, 70, 6]$ erhält man durch Einschränkung auf die ersten 81 Spalten und 11 Zeilen.

```
131222233221310113212110132030111102112231102332231213321000000000032322130202310
220033301231301303010121332221022311123000211013211013020100000000012021033023300
202003330123130133001012133220223121110230021102113101230010000000021223201321130
012133022320233210023321000332013221331211201002210031220001000000032231021113020
213120013100103123221112313020110011311003323011210322320000100000023111212021210
122203123203220003313221110321133310201033033123032100030000010000001310121233210
102220312320322030031322111031233131020013303310323210300000001000011101011010320
223333113321202132232202130122002232231322031112333213210000000100000011001211220
220103310000020112203021020103330302300321223303011112010000000010000000102230210
233102233132101000113010212221301220031122012322011022110000000001000000011110120
223012100213230202000310211120011103321303230302103301320000000000100000000001110
000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
202133122132001322230121 22
101233302013210013031221 30
201131003333313121111332 31
201020320021001332201131 02
200110112030331030321023 33
300001102212101312020211 02
000000011200101132003013 21
200000000011100101220333 03
100000000000011123330313 13
300000000000000000011100 33
100000000000000000001233 33
011111111111111111111111 11
```

Checkmatrix eines quaternären $[70, 57, 7]$

```
10000000000003231022111202301220303321001200200121302033303323323020 20
01000000000002331310200211323201222032303210110322121120022033032002 31
00100000000001010301120112320223033222032211321223101202013221321120 21
00010000000030131102123333033200303313021013120111223102323331233212 0
00001000000003213231321111201030330020031130311332320001010222301112 12
00000100000000321323132111120103033002003113031133232000101022232111 33
00000010000001211302213322300113212321002221033302030110001120202331 02
00000001000000121130221332230011321232100222103330203011000112020220 31
00000000100003100033322211312303201130311302030200212131133000210113 02
00000000010002021313132030212031102121332320313302100333131333011213 12
00000000001002133221113012302002332220230022121012331113331100332021 30
00000000000101030112011232022303322203221132122310120201322132010322 01
00000000000012232301001332121031110212021303302113131310011022023133223
```

Erzeugermatrix eines quaternären $[43, 12, 19]$

$$
\begin{array}{l}
10000000000023313102002113232012220323032 10 \\
01000000000010103011201123202230332220322 11 \\
00100000000030131102123333033200303313021 01 \\
00010000000032132313211112010303300200311 30 \\
00001000000003213231321111201030330020031 13 \\
00000100000001211302213322300113212321002 21 \\
00000010000001211302213322300113212321002 22 \\
00000001000031000333222113123032011303113 02 \\
00000000100020213131320302120311021213323 20 \\
00000000010021332211301230200233222023002 2 \\
00000000001010301120112320223033222032211 32 \\
00000000000122323010013321210311102120213 03
\end{array}
$$

C Verzeichnis der linearen Codes

C.1 binäre Codes

Alle Codes ungerader Distanz wurden durch einen parety Check ergänzt.

Code	Seite
[155, 132, 8]	67
[162, 138, 8]	67
[266, 240, 8]	48
[275, 248, 8]	49
[277, 249, 8]	49
[280, 250, 8]	49
[287, 255, 8]	48
[72, 46, 10]	67
[266, 232, 10]	48
[265, 223, 12]	39
[273, 230, 12]	39
[275, 231, 12]	45
[279, 233, 12]	49
[286, 238, 12]	39
[39, 12, 14]	67
[76, 39, 14]	38
[265, 215, 14]	34
[265, 207, 16]	39
[273, 214, 16]	39
[278, 216, 16]	45
[280, 217, 16]	39
[286, 222, 16]	39
[265, 199, 18]	34
[143, 79, 20]	36
[145, 80, 20]	36
[147, 81, 20]	36
[261, 191, 20]	39
[264, 192, 20]	45
[266, 193, 20]	45
[272, 198, 20]	39
[274, 199, 20]	39
[149, 78, 22]	38
[152, 79, 22]	45
[154, 80, 22]	45
[265, 187, 22]	39
[269, 190, 22]	39
[271, 191, 22]	45
[274, 192, 22]	45
[280, 197, 22]	39
[145, 71, 24]	38
[265, 179, 24]	39
[273, 186, 24]	39
[275, 187, 24]	45
[278, 188, 24]	45
[280, 189, 24]	39
[265, 171, 26]	39
[273, 178, 26]	39
[275, 179, 26]	45
[278, 180, 26]	45
[280, 181, 26]	39
[143, 58, 28]	36
[145, 59, 28]	36
[147, 60, 28]	36
[265, 163, 28]	39
[273, 170, 28]	39
[275, 171, 28]	45
[278, 172, 28]	45
[280, 173, 28]	39
[149, 57, 30]	38
[265, 155, 30]	39
[273, 162, 30]	39
[275, 163, 30]	45
[278, 164, 30]	45
[280, 165, 30]	39
[90, 18, 32]	36
[132, 44, 32]	47
[136, 47, 32]	47
[140, 50, 32]	47
[145, 51, 32]	47
[148, 52, 32]	47
[152, 55, 32]	47
[211, 97, 32]	73
[265, 147, 32]	40
[273, 154, 32]	40
[275, 155, 32]	45
[278, 156, 32]	45
[78, 10, 34]	59
[133, 37, 34]	73
[143, 43, 34]	47
[259, 135, 34]	34
[136, 37, 36]	73
[144, 40, 36]	47
[148, 43, 36]	47
[260, 134, 36]	34
[84, 10, 38]	60
[139, 33, 38]	73
[146, 38, 38]	47
[152, 43, 38]	47
[87, 10, 40]	60
[133, 30, 40]	73

Code	Seite
[155, 19, 60]	39
[158, 21, 60]	39
[160, 22, 60]	39
[165, 23, 60]	45
[170, 25, 60]	45
[172, 26, 60]	45
[178, 29, 60]	39
[208, 41, 60]	73
[218, 45, 60]	73
[153, 16, 62]	37
[161, 18, 62]	37
[163, 19, 62]	37
[166, 21, 62]	39
[168, 22, 62]	39
[216, 41, 62]	73
[233, 49, 62]	73
[241, 53, 62]	73
[262, 72, 62]	47
[265, 73, 62]	47
[268, 75, 62]	47
[156, 16, 64]	37
[164, 18, 64]	37
[265, 71, 64]	47
[154, 14, 66]	39
[156, 15, 66]	39
[217, 37, 66]	73
[257, 57, 66]	73
[158, 14, 68]	39
[160, 15, 68]	39
[162, 14, 70]	39
[164, 15, 70]	39
[159, 12, 72]	58
[165, 14, 72]	39
[167, 15, 72]	39
[155, 8, 76]	34
[171, 11, 78]	59
[168, 8, 82]	34
[177, 11, 82]	59
[171, 8, 84]	34
[180, 11, 84]	59
[175, 8, 86]	34
[183, 11, 86]	59
[178, 8, 88]	34
[186, 11, 88]	59
[259, 47, 88]	40

Code	Seite
[186, 9, 90]	59
[189, 11, 90]	59
[202, 15, 90]	61
[265, 45, 90]	34
[192, 11, 92]	59
[206, 15, 92]	61
[258, 38, 92]	34
[193, 9, 94]	60
[196, 11, 94]	60
[205, 13, 94]	61
[210, 15, 94]	61
[196, 9, 96]	60
[199, 11, 96]	60
[213, 15, 96]	61
[258, 30, 96]	34
[203, 9, 98]	60
[207, 11, 98]	62
[210, 11, 100]	62
[211, 9, 102]	60
[214, 11, 102]	62
[214, 9, 104]	60
[217, 11, 104]	62
[258, 22, 104]	34
[221, 11, 106]	62
[221, 9, 108]	60
[224, 11, 108]	63
[228, 11, 110]	63
[228, 9, 112]	60
[231, 11, 112]	63
[235, 9, 114]	64
[238, 10, 114]	64
[240, 11, 114]	64
[242, 10, 116]	64
[244, 11, 116]	64
[246, 10, 118]	60
[249, 11, 118]	64
[246, 9, 120]	60
[249, 10, 120]	60
[254, 10, 122]	63
[258, 11, 122]	64
[257, 10, 124]	64
[261, 10, 126]	34

C.2 ternäre Codes

Code	Seite
$[57, 15, 21]$	80
$[82, 35, 21]$	35
$[86, 37, 21]$	41
$[89, 39, 21]$	41
$[125, 68, 21]$	35
$[129, 71, 21]$	35
$[56, 14, 22]$	74
$[84, 35, 22]$	41
$[114, 56, 22]$	74
$[130, 69, 22]$	76
$[133, 71, 22]$	42
$[56, 13, 23]$	74
$[84, 34, 23]$	41
$[88, 35, 23]$	46
$[92, 38, 23]$	41
$[127, 66, 23]$	35
$[129, 67, 23]$	74
$[131, 68, 23]$	42
$[135, 71, 23]$	42
$[58, 13, 24]$	80
$[67, 18, 24]$	74
$[85, 32, 24]$	41
$[87, 33, 24]$	41
$[89, 34, 24]$	41
$[115, 53, 24]$	80
$[68, 17, 25]$	74
$[72, 19, 25]$	74
$[88, 31, 25]$	41
$[115, 51, 25]$	76
$[118, 53, 25]$	76
$[122, 56, 25]$	76
$[115, 50, 26]$	74
$[120, 53, 26]$	74
$[124, 56, 26]$	76
$[114, 47, 27]$	74
$[120, 51, 27]$	76
$[124, 54, 27]$	76
$[128, 57, 27]$	76
$[116, 47, 28]$	80
$[118, 48, 28]$	80
$[121, 50, 28]$	76
$[115, 44, 29]$	74
$[121, 48, 29]$	76
$[125, 51, 29]$	76
$[58, 10, 30]$	40
$[117, 44, 30]$	80
$[77, 17, 31]$	74
$[86, 21, 31]$	74
$[120, 44, 31]$	76
$[123, 46, 31]$	76
$[115, 40, 32]$	74

Code	Seite
$[80, 17, 33]$	74
$[86, 19, 33]$	80
$[88, 20, 33]$	80
$[114, 37, 33]$	74
$[119, 40, 33]$	74
$[122, 42, 33]$	76
$[121, 40, 34]$	80
$[83, 17, 35]$	74
$[87, 18, 35]$	80
$[92, 20, 35]$	74
$[94, 21, 35]$	76
$[96, 22, 35]$	76
$[114, 34, 35]$	74
$[119, 37, 35]$	74
$[122, 39, 35]$	76
$[125, 41, 35]$	76
$[94, 20, 36]$	74
$[121, 37, 36]$	80
$[86, 17, 37]$	74
$[90, 18, 37]$	80
$[96, 20, 37]$	74
$[98, 21, 37]$	76
$[100, 22, 37]$	76
$[119, 34, 37]$	74
$[122, 36, 37]$	76
$[125, 38, 37]$	76
$[128, 40, 37]$	76
$[94, 19, 38]$	80
$[115, 31, 38]$	74
$[121, 34, 38]$	80
$[89, 17, 39]$	74
$[93, 18, 39]$	80
$[96, 19, 39]$	80
$[99, 20, 39]$	80
$[102, 21, 39]$	46
$[122, 33, 39]$	74
$[125, 35, 39]$	76
$[95, 18, 40]$	80
$[98, 19, 40]$	80
$[101, 20, 40]$	80
$[115, 28, 40]$	74
$[92, 17, 41]$	74
$[97, 18, 41]$	80
$[100, 19, 41]$	80
$[109, 24, 41]$	41
$[112, 25, 41]$	74
$[115, 26, 41]$	80
$[125, 33, 41]$	74
$[127, 34, 41]$	80
$[129, 35, 41]$	76
$[131, 36, 41]$	35

Code	Seite
$[123, 16, 63]$	35
$[127, 15, 65]$	35
$[129, 16, 65]$	42
$[104, 7, 66]$	64
$[108, 7, 69]$	64
$[123, 11, 69]$	35
$[132, 15, 69]$	35
$[134, 16, 69]$	42
$[129, 11, 71]$	42
$[112, 7, 72]$	65
$[118, 7, 74]$	65
$[120, 7, 75]$	65
$[134, 11, 75]$	42
$[123, 7, 77]$	65
$[125, 7, 78]$	41
$[129, 7, 81]$	46

C.3 quaternäre Codes

Code	Seite
$[72, 27, 25]$	35
$[77, 28, 25]$	80
$[79, 29, 25]$	80
$[82, 31, 25]$	78
$[85, 33, 25]$	78
$[89, 36, 25]$	78
$[122, 63, 25]$	78
$[70, 24, 26]$	46
$[81, 29, 26]$	78
$[87, 33, 26]$	75
$[91, 36, 26]$	78
$[117, 57, 26]$	78
$[69, 23, 27]$	43
$[74, 26, 27]$	43
$[76, 27, 27]$	46
$[80, 28, 27]$	75
$[86, 31, 27]$	75
$[89, 33, 27]$	78
$[93, 36, 27]$	78
$[67, 20, 28]$	43
$[71, 22, 28]$	43
$[73, 23, 28]$	43
$[76, 25, 28]$	43
$[78, 26, 28]$	43
$[80, 27, 28]$	46
$[88, 31, 28]$	80
$[91, 33, 28]$	78
$[126, 61, 28]$	78
$[69, 19, 29]$	43
$[71, 20, 29]$	43
$[75, 22, 29]$	43
$[77, 23, 29]$	46
$[80, 25, 29]$	43
$[82, 26, 29]$	46
$[84, 27, 29]$	35
$[86, 28, 29]$	75
$[70, 18, 30]$	46
$[96, 34, 30]$	78
$[100, 37, 30]$	78
$[104, 40, 30]$	78
$[69, 17, 31]$	43
$[74, 20, 31]$	43
$[78, 22, 31]$	43
$[80, 23, 31]$	46
$[83, 25, 31]$	43
$[87, 27, 31]$	35
$[91, 29, 31]$	78
$[98, 34, 31]$	78
$[102, 37, 31]$	78
$[83, 23, 32]$	75
$[90, 27, 32]$	78

Code	Seite
$[93, 29, 32]$	78
$[87, 24, 33]$	75
$[89, 25, 33]$	78
$[92, 27, 33]$	78
$[99, 32, 33]$	78
$[109, 38, 34]$	78
$[113, 41, 34]$	78
$[88, 23, 35]$	75
$[90, 24, 35]$	80
$[92, 25, 35]$	78
$[94, 26, 35]$	78
$[97, 28, 35]$	78
$[124, 48, 35]$	78
$[53, 6, 36]$	42
$[90, 23, 36]$	80
$[94, 25, 36]$	75
$[103, 31, 36]$	78
$[110, 36, 36]$	79
$[88, 20, 37]$	75
$[116, 39, 37]$	79
$[120, 42, 37]$	79
$[101, 27, 38]$	75
$[111, 34, 38]$	79
$[104, 28, 39]$	79
$[107, 30, 39]$	79
$[110, 32, 39]$	79
$[117, 37, 39]$	79
$[121, 40, 39]$	79
$[101, 25, 40]$	75
$[103, 26, 40]$	79
$[106, 28, 40]$	79
$[116, 35, 40]$	79
$[127, 43, 40]$	79
$[122, 38, 41]$	79
$[103, 24, 42]$	75
$[105, 25, 42]$	79
$[108, 27, 42]$	79
$[111, 29, 42]$	79
$[128, 41, 42]$	79
$[103, 23, 43]$	75
$[105, 24, 43]$	79
$[113, 28, 44]$	79
$[116, 30, 44]$	79
$[104, 22, 45]$	75
$[108, 24, 45]$	75
$[110, 25, 45]$	79
$[70, 8, 46]$	46
$[106, 22, 46]$	75
$[110, 24, 46]$	75
$[115, 27, 46]$	75
$[121, 31, 46]$	79

Code	Seite
$[124, 33, 46]$	79
$[121, 30, 47]$	75
$[70, 7, 48]$	43
$[73, 8, 48]$	43
$[123, 30, 48]$	75
$[126, 32, 48]$	79
$[129, 34, 48]$	79
$[117, 25, 49]$	79
$[75, 7, 50]$	46
$[77, 8, 50]$	35
$[117, 24, 50]$	75
$[125, 29, 50]$	79
$[128, 31, 50]$	79
$[122, 26, 51]$	75
$[130, 30, 52]$	79
$[125, 26, 53]$	75
$[130, 28, 54]$	75
$[97, 8, 63]$	46
$[95, 6, 66]$	35

Literatur

[1] W.O. Alltop: *A method for extending binary linear codes,* IEEE Transactions on Information Theory. 30 (1984), 871-872.

[2] D. Augot, P. Charpin, N. Sendrier: *Studying the locator polynomials of minimum weight codewords of BCH codes,* IEEE Transactions on Information Theory 38 (1992), 960-973.

[3] J. Bierbrauer: *Construction of orthogonal arrays,* Journal of Statistical Planning and Inference 56 (1996) 39-42.

[4] J. Bierbrauer, Y. Edel: *New code parameters from Reed-Solomon subfield codes,* IEEE Transactions on Information Theory 43 (1997),953-968.

[5] J. Bierbrauer, Y. Edel: *Extending and lengthening BCH-codes,* erscheint in: *Finite Fields and their Applications.*

[6] J. Bierbrauer, Y. Edel: *Dense sphere packings from new codes,* erscheint in: Proceedings.

[7] J. Bierbrauer, Y. Edel: *A family of 2-weight codes related to BCH-codes,* eingereicht bei: Journal of Combinatorial Designs.

[8] A.E. Brouwer: *Data base of bounds for the minimum distance for binary, ternary and quaternary codes,*
URL http://www.win.tue.nl/win/math/dw/voorlincod.html oder
URL http://www.cwi.nl/ht/aeb/lincodbd/2/136/114 oder
URL ftp://ftp.win.tue.nl/pub/math/codes/tabel[234].gz

[9] A.E. Brouwer,T. Verhoeff: *An updated table of minimum-distance bounds for binary linear codes,* IEEE Transactions on Information Theory 33 (1987), 719-721.

[10] R. Calderbank, W.M. Kantor: *The geometry of two weight-codes,* Bull.London Math.Soc (1986), 97-122.

[11] Y. Cheng: *New linear Codes Constructed by Concatenation, Extending, and Shortening Methods,* IEEE Transactions on Information Theory 39 (1993), 662-677.

[12] J.H. Conway, N.J.A. Sloane : *Sphere Packings, Lattices and Groups,* (2nd ed.) Springer-Verlag Berlin (1993).

[13] P. Delsarte: *Bounds for unrestricted codes, by linear programming,* Philips Research Reports 27 (1972), 272-289.

[14] P. Delsarte: *Four fundamental parameters of a code and their combinatorial significance,* Information and Control 23 (1973), 407-438.

[15] P. Delsarte: *On Subfield Subcodes of Modified Reed-Solomon Codes,* IEEE Transactions on Information Theory 21 (1975), 575-576.

[16] Y. Edel, J. Bierbrauer: *Lengthening and the Gilbert-Varshamov bound,* IEEE Transactions on Information Theory 43 (1997), 991-992.

[17] Y. Edel, J. Bierbrauer: *Twisted BCH-codes,* eingereicht bei: Journal of Combinatorial Designs.

[18] Y. Edel, J. Bierbrauer: *Some codes related to BCH-codes of low dimension,* Manuskript.

[19] J.H. Griesmer: *A bound for error correcting codes,* IBM Journal Research Development 4 (1960), 532-542.

[20] B. Groneick, S. Grosse: *New binary codes,* IEEE Transactions on Information Theory 40 (1994), 510-512.

[21] T. Kasami, N. Tokura: *Some remarks on BCH bounds and minimum weights of binary primitive BCH codes,* IEEE Transactions on Information Theory 15 (1969), 408-413.

[22] J.H. van Lint: *Introduction to Coding Theory,* (2nd ed.) Springer-Verlag Berlin (1992).

[23] F.J. MacWilliams: *A Theorem on the distribution of weights in a systematic code,* Bell Syst. Tech. J. 42 (1963) 79-94.

[24] F.J. MacWilliams, N.J.A. Sloane: *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam (1977).

[25] L. Rédei: *Lückenhafte Polynome,* Birkhäuser Verlag, Basel, Stuttgart 1970.

[26] W.Ch. Schmid, R. Wolf: *Bounds on digital nets and sequences,* Manuskript (Institut für Mathematik Universität Salzburg).

[27] H. Stichtenoth: *Algebraic Function Fields and Codes,* Springer-Verlag Berlin (1993).