Quadratische Restcodes

Vortrag zum Seminar „Gitter und Codes“

Paul Rohrbach

18.05.2015

Einleitung

Dieser Vortrag behandelt verschiedene Konstruktionen von Codes und deren Eigenschaften. Die Grundkonstruktion der hier vorgestellten Codes ist die der zyklischen Codes. Diese haben als strukturell bestimmende Eigenschaft, dass man jedes Codewort zyklisch durchtauschen kann und wieder ein Element des Codes erhält.

Nach einer anfänglichen Charakterisierung werden wir zwei Typen von zyklischen Codes genauer betrachten: die BCH-Codes und darauf aufbauend die Klasse der quadratischen Restcodes. Diese Spezialisierungen ermöglichen es, Aussagen über den Minimalabstand und die Automorphismengruppe zu treffen, die für allgemeine zyklische Codes sehr schwierig sind.

Der Vortrag folgt größtenteils Abschnitt 2.10 des Buches *Lattices and Codes* von Wolfgang Ebeling [2].

1 Zyklische Codes

Zunächst wollen wir uns mit allgemeinen zyklischen Codes beschäftigen. Ziel dieses Abschnittes ist es, eine vollständige Konstruktion für solche Codes zu finden.

Definition 1.1 *Sei K ein Körper und C ein linearer Code der Länge $n \in \mathbb{N}$ über K. Dann nennt man C* ***zyklisch****, falls für ein Codewort $(c_0, c_1, \ldots, c_{n-1}) \in C$ auch $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ Element des Codes C ist.*

Die Konstruktion solcher Codes erfolgt durch Polynome über endlichen Körpern. Daher benötigen wir einige Aussagen zu endlichen Körpern und dem Verhalten von Polynomen über diesen.

Für eine Primzahl $p \in \mathbb{N}$ ist der endliche Körper der Ordnung p eindeutig gegeben durch $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Ist $\mathbb{F}_q$ ein Körper mit q Elementen, so ist q die Potenz einer Primzahl p, also $q = p^r$ mit $r \in \mathbb{N}$. Es gilt, dass $\mathbb{F}_q$ Charakteristik p hat, $\mathbb{F}_p$ als Teilkörper enthält und die Einheitengruppe $\mathbb{F}_q^*$ zyklisch mit $q-1$ Elementen ist. Ein Element $\alpha \in \mathbb{F}_q$ heißt primitive n-te Einheitswurzel, wenn $\alpha^n = 1$ und $\alpha^i \neq 1$ für alle $0 < i < n$ ist.

Die Abbildung $\sigma : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^p$ ist ein Körperautomorphismus, der die Elemente des Teilkörpers $\mathbb{F}_p$ fest lässt. Diese Abbildung wird Frobeniusautomorphismus genannt. Es gilt $\sigma^r = 1$. Der Frobeniusautomorphismus erzeugt eine zyklische Gruppe der Ordnung r von Abbildungen, die $\mathbb{F}_p$ fest lassen, diese wird Galois-Gruppe genannt. Das Polynom $x^q - x$ ist das Produkt der normierten, irreduziblen Polynome in $\mathbb{F}_p[x]$ von Grad s mit

s teilt r. Die Bahnen der Operation der Galois-Gruppe auf $\mathbb{F}_q$ über $\mathbb{F}_p$ sind genau die Nullstellen der irreduziblen Faktoren von $x^q - x$.

Beispiel 1.2 *Sei $p = 2$ und $q = 2^3$. Dann kann man den Körper mit 2^3 Elementen konstruieren durch $\mathbb{F}_8 = \mathbb{F}_2[z]/(z^3 + z + 1)$. Die Einheitengruppe von $\mathbb{F}_p$ hat 7 Elemente. Da 7 prim ist, ist $\alpha := z \neq 1$ ein Erzeuger der Einheitengruppe.*

Die Bahnen der Operation der Galois-Gruppe sind gegeben durch

$$\{1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}.$$

Also hat das Minimalpolynom von α, das kleinste normierte Polynom in $\mathbb{F}_2[x]$, welches α als Wurzel hat, die Form $\mu_\alpha = (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1 \in \mathbb{F}_2[x]$.

Für ein $n \in \mathbb{N}$ mit $\mathrm{ggT}(n, p) = 1$ betrachten wir nun das Polynom $x^n - 1$. Dann bilden die Polynome $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ mit $a_i \in \mathbb{F}_q$, $1 \leq i \leq n - 1$, ein Vertretersystem des Faktorrings $\mathbb{F}_q[x]/(x^n - 1)$. Daher identifizieren wir $\mathbb{F}_q[x]/(x^n - 1)$ mit $\mathbb{F}_q^n$ durch Abbilden der Vertreter $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ auf das n-Tupel $(a_0, a_1, \ldots, a_{n-1})$.

Satz 1.3 *Durch eine Zerlegung $x^n - 1 = g(x)h(x)$ mit $g(x), h(x) \in \mathbb{F}_q[x]$ und $\deg(g) = m < n$ erhält man den linearen Code*

$$C = \{a(x)g(x) \pmod{x^n - 1} \mid a(x) \in \mathbb{F}_q[x]\} \subset \mathbb{F}_q^n .$$

Dieser Code hat Länge n, Dimension $n - m$ und ist zyklisch. Weiter existiert zu jedem zyklischen Code ein äquivalenter Code dieser Darstellung.

Beweis C ist das von $g(x)$ erzeugte Ideal in $\mathbb{F}_q[x]$ modulo $(x^n - 1)$ und damit insbesondere abgeschlossen unter Skalarmultiplikation und Addition, also ist C linear. Nach Voraussetzung teilt $g(x)$ das Polynom $x^n - 1$ und damit ist $(x^n - 1)\,\mathbb{F}_q[x]$ eine Teilmenge von $g(x)\,\mathbb{F}_q[x]$. Also ist C als $\mathbb{F}_q$-Vektorraum isomorph zu $\mathbb{F}_q[x]/\langle h(x)\rangle$ und hat Dimension $n - m$.

Sei $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in C$. Da $x^n \equiv 1 \pmod{x^n - 1}$ folgt

$$xc(x) = c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n \equiv c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1} \pmod{x^n - 1},$$

also ist C zyklisch nach Definition (1.1).

Sei nun $C \leq \mathbb{F}_q^n$ ein linearer, zyklischer Code. Betrachtet man ein Codewort $c \in C$ als Polynom $c(x)$ in $\mathbb{F}_q[x]$ vom Grad kleiner n, so folgt mit obiger Argumentation, dass auch $xc(x) \pmod{x^n - 1}$ wieder in C liegt. Damit ist $C + (x^n - 1)\,\mathbb{F}_q[X]$ abgeschlossen unter Multiplikation mit Polynomen, also auch ein Ideal in $\mathbb{F}_q[x]$. Da $\mathbb{F}_q[x]$ ein Hauptidealbereich ist, existiert ein $g(x) \in \mathbb{F}_q[x]$ welches das Ideal erzeugt. Damit gilt

$$C = \{a(x)g(x) \pmod{x^n - 1} \mid a(x) \in \mathbb{F}_q[x]\},$$

also ist C der von $g(x)$ erzeugte zyklische Code. ∎

Man bezeichnet $g(x)$ als das Erzeugerpolynom von C. Mit den Koeffizienten von $g(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$, wobei $b_{m+1} = \cdots = b_{n-1} = 0$, ist die Erzeuger-Matrix von C gegeben durch

$$\begin{pmatrix} b_0 & b_1 & \dots & b_{n-1} \\ b_{n-1} & b_0 & \dots & b_{n-2} \\ \vdots & \vdots & \dots & \vdots \\ b_m & b_{m+1} & \dots & b_{m-1} \end{pmatrix} \in \mathbb{F}_q^{(n-m)\times n}.$$

In zyklischen Codes existiert immer mindestens ein vom Nullwort verschiedenes Idempotent. Es existiert weiter genau ein Idempotent, welches gleichzeitig noch eine Eins des Codes ist und diesen erzeugt. Es kann also als Alternative zum Erzeugerpolynom zur Konstruktion eines (linearen) Erzeugendensystems benutzt werden. Diese Eigenschaft werden wir später benötigen.

Satz 1.4 *Ein Codewort $c(x)$ des zyklischen Codes C heißt idempotent, falls gilt*

$$c^2(x) = c(x).$$

In einem zyklischen Code existiert genau ein Idempotent, das auch eine Eins des Codes ist. Dieses Wort ist ein weiterer Erzeuger des Codes.

Beweis Das Polynom $x^n - 1$ zerfällt in paarweise verschiedene irreduzible Faktoren, denn mit einem mehrfach auftretenden Faktor $f \in \mathbb{F}_q[x]$ mit $\deg(f) > 1$ könnte man $x^n - 1$ faktorisieren zu

$$x^n - 1 = f^2 r \text{ für ein } r \in \mathbb{F}_q[x].$$

Formales Ableiten liefert

$$nx^{n-1} = 2ff'r + f^2r' = f(2f'r + fr')$$

und es folgt f teilt $\mathrm{ggT}(nx^{n-1}, x^n - 1)$. Für $\mathrm{ggT}(n, p) = 1$ gilt aber $\mathrm{ggT}(nx^{n-1}, x^n - 1) = 1$ und man erhält einen Widerspruch.

Also sind $g(x)$ und $h(x)$ teilerfremd und nach dem chinesischen Restsatz ist die Abbildung

$$\varphi : \mathbb{F}_q[x]/\langle x^n - 1\rangle \to \mathbb{F}_q[x]/\langle g(x)\rangle \oplus \mathbb{F}_q[x]/\langle h(x)\rangle,\ x \mapsto (x + \langle g(x)\rangle, x + \langle h(x)\rangle)$$

ein Isomorphismus. Es ist $c(x) := \varphi^{-1}((0,1))$ ein idempotentes Codewort, welches auch die eindeutige Eins von C ist. Es folgt $b(x)c(x) = b(x)$ für alle $b(x) \in C$ und damit ist $c(x)$ ein weiterer Erzeuger des Codes. ∎

2 BCH-Codes

Es ist schwierig, für allgemeine zyklische Codes Aussagen über den Minimalabstand zu bekommen. Daher ist das Ziel dieses Kapitels zusätzliche Bedingungen an den Code zu stellen, um den Minimalabstand zumindest abschätzen zu können.

Als einführendes Beispiel betrachten wir einen bekannten perfekten Code, den $[7, 4, 3]$-Hamming-Code H über dem $\mathbb{F}_2$. Eine Bildtestmatrix, welche den Code eindeutig bestimmt, hat dann die Form

$$B := \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{3\times 7}.$$

Jetzt wollen wir die Ideen von Kapitel 1 benutzen, um diesen Code zu untersuchen. Man kann die Elemente von $\mathbb{F}_2^3$ auch als Elemente in $\mathbb{F}_{2^3} = \mathbb{F}_2[z]/(z^3 + z + 1)$ über die Identifikation mit den Polynomkoeffizienten betrachten. Es ist $\alpha := z$ ein zyklischer Erzeuger der Einheitengruppe $\mathbb{F}_{2^3}^*$, also eine primitive 7. Einheitswurzel. Damit erreichen wir eine Darstellung der Bildtestmatrix durch Potenzen von α und erhalten hier

$$B = \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix} \in \mathbb{F}_{2^3}^{1\times 7}.$$

Ein Wort $c \in \mathbb{F}_2^7$ liegt also genau dann im Code, wenn $Bc = c_0\alpha_0 + c_1\alpha_1 + \cdots + c_6\alpha^6 = 0$. Betrachtet man c als Polynom in $\mathbb{F}_2[x]$ vom Grad ≤ 6, so erhält man, dass $c(x) \in \mathbb{F}_2[x]$ genau dann ein Element des Codes ist, wenn $c(\alpha) = 0$ gilt.

Das Minimalpolynom μ_α von α, das kleinste normierte Polynom in $\mathbb{F}_2[x]$ welches α als Wurzel hat, teil $x^7 - 1$. Also kann man den Code als Ideal in $\mathbb{F}_2[x]$ modulo $x^7 - 1$ darstellen und erhält mit $g(x) := \mu_\alpha$

$$\begin{aligned} H &\cong \{c(x) \in \mathbb{F}_2[x]_{\text{Grad} \leq 7} \mid c(\alpha) = 0\} \\ &= \{c(x) \in \mathbb{F}_2[x]_{\text{Grad} \leq 7} \mid g(x) \text{ teilt } c(x)\} \\ &\cong \{a(x)g(x) \pmod{x^7 - 1} \mid a(x) \in \mathbb{F}_2[x]\}. \end{aligned}$$

H ist genau der von $g(x)$ erzeugte zyklische Code. Das Minimalpolynom ist der irreduzible Faktor von $x^7 - 1$ mit Wurzel α, daher das Produkt der Linearfaktoren zu den Elementen der Bahn von α unter der Operation der Galois-Gruppe. Nach Beispiel (1.2) folgt $g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1 \in \mathbb{F}_2$.

Es stellt sich die Frage, wie man den Minimalabstand des Codes verbessern kann, wenn man weitere Zeilen in die Bildtestmatrix einfügt, also welches $\beta \in \mathbb{F}_{2^3}$ man zum Beispiel wählen sollte, so dass der durch die Bildtestmatrix

$$H' := \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \beta^0 & \beta^1 & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \end{pmatrix}$$

gegebene Code einen höheren Minimalabstand hat.

Eine mögliche Wahl dieser Elemente wurde von R. C. Bose, D. K. Ray-Chaudhuri und A. Hocquenghem untersucht.

Definition 2.1 *Sei α eine primitive n-te Einheitswurzel in $\mathbb{F}_q$. Dann nennt man den von*

$$g(x) := \mathrm{kgV}(\mu_\alpha, \mu_{\alpha^2}, \ldots, \mu_{\alpha^r}) \in \mathbb{F}_p[x]$$

*erzeugten Code C einen **BCH-Code** mit designiertem Minimalgewicht von $r+1$.*

Durch Verwendung der Minimalpolynome erhält man einen Code über dem Primkörper $\mathbb{F}_p$. Es bleibt zu zeigen, dass das designierte Minimalgewicht auch erreicht wird. Dazu zeigen wir folgende leichte Verallgemeinerung.

Satz 2.2 *Sei $x^n - 1 = g(x)h(x)$ mit $g(x), h(x) \in \mathbb{F}_q[x]$. Gilt*

$$(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^r) \text{ teilt } g(x),$$

*so hat der von $g(x)$ erzeugte Code ein Minimalgewicht von größer gleich $r+1$. Diese untere Schranke wird auch **BCH-Schranke** genannt.*

Beweis Angenommen der Minimalabstand ist kleiner gleich r. Dann existiert ein Codewort $c(x)$ in C mit Gewicht $0 < w(c) \leq r$ mit $c(x) = a_{t_1}x^{t_1} + \cdots + a_{t_r}x^{t_r}$ in C mit t_i paarweise verschiedenen Zahlen $0 \leq t_i \leq n-1$ für $i = 1, \ldots, r$.

Nach Wahl des Erzeugerpolynoms gilt $(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^r)$ teilt $c(x)$ und damit

$$\begin{aligned} c(\alpha) &= a_{t_1}\alpha^{t_1} + \cdots + a_{t_r}\alpha^{t_r} &&= 0 \\ c(\alpha^2) &= a_{t_1}\alpha^{2t_1} + \cdots + a_{2t_r}\alpha^{t_r} &&= 0 \\ &\vdots && \vdots \\ c(\alpha^r) &= a_{t_1}\alpha^{rt_1} + \cdots + a_{t_r}\alpha^{rt_r} &&= 0. \end{aligned}$$

Dies ist ein lineares Gleichungssystem in $a_{t_1}, \ldots, a_{t_r}$. Betrachtet man die Determinante der Koeffizientenmatrix, so erhält man durch Benutzen der Multilinearität und der Berechnungsvorschrift für Determinanten von Vandermonde-Matrizen

$$\begin{aligned} \det \begin{pmatrix} \alpha^{t_1} & \ldots & \alpha^{t_r} \\ \alpha^{2t_1} & \ldots & \alpha^{2t_r} \\ \vdots & \ddots & \vdots \\ \alpha^{rt_1} & \ldots & \alpha^{rt_r} \end{pmatrix} &= \alpha^{t_1}\cdots\alpha^{t_r} \det \begin{pmatrix} 1 & \ldots & 1 \\ \alpha^{t_1} & \ldots & \alpha^{t_r} \\ \vdots & \ddots & \vdots \\ \alpha^{(r-1)t_1} & \ldots & \alpha^{(r-1)t_r} \end{pmatrix} \\ &= \pm\alpha^{t_1}\cdots\alpha^{t_r} \cdot \prod_{i<j}(\alpha^{t_i} - \alpha^{t_j}). \end{aligned}$$

Da für n-te Einheitswurzeln insbesondere $0 \neq \alpha^i \neq \alpha^j$ für alle $i, j \in \{1, \ldots, n-1\}$ mit $i \neq j$ gilt, ist die Determinante ungleich Null und die einzige Lösung

$$a_{t_1} = a_{t_2} = \cdots = a_{t_{n-1}} = 0,$$

was im Widerspruch zu $w(c) > 0$ steht. ∎

Um mit dieser Methode auch Codes über Teilkörpern, insbesondere dem $\mathbb{F}_2$, zu bekommen, benutzt man folgende Eigenschaft: Ist K_0 ein Teilkörper von $\mathbb{F}_q$ und $g(x)$ auch ein Polynom in K_0, so kann man die obige Konstruktion analog über K_0 betrachten. Der so konstruierte lineare Code $C \subset K_0^n$ hat ebenfalls Dimension $n - m$ über K_0.

Für Codes über dem $\mathbb{F}_2$ wollen wir jetzt den Dualcode konstruieren. Sei dazu $x^n - 1 = g(x)h(x)$ in $\mathbb{F}_2[x]$, wobei n ungerade ist. Wir bezeichnen mit C_g den von $g(x)$ erzeugten zyklischen Code.

Lemma 2.3 *Der Dualcode $C_g^\perp$ ist äquivalent zum zyklischen Code $C_{\tilde{h}}$ mit*

$$\tilde{h}(x) \equiv x^{\deg h} h(x^{-1}) \pmod{x^n - 1}.$$

BEWEIS Da $g(x)h(x) = x^n - 1$, hat sowohl $g(x)$ als auch $h(x)$ einen von Null verschiedenen konstanten Anteil. Damit folgt $\deg \tilde{h} = \deg h$ sowie $\deg g + \deg h = n$ und $\dim C_g + \dim C_{\tilde{h}} = n$ nach Voraussetzung.

Für zwei Elemente $a(x), b(x) \in \mathbb{F}_2[x]/\langle x^n - 1\rangle$ ist das innere Produkt $a \cdot b = \sum_{i=1}^n a_i b_i$ genau der konstante Anteil von $a(x)b(x^{-1})$. Da

$$g(x)\tilde{h}(x^{-1}) = g(x)h(x)x^{-\deg h} = (x^n - 1)x^{m-n}$$

konstanten Term Null hat, folgt insbesondere $C_{\tilde{h}} \subset C_g^\perp$ und damit die Aussage aus Dimensionsgründen. ∎

Haben in einem Code C der Dimension n alle von Null verschiedenen Codewörter das selbe Gewicht d, so spricht man von einem Simplex-Code. Der Gewichtszähler dieses Codes ist dann von der Form

$$W_c(X, Y) = X^n + aX^{n-d}Y^d$$

mit $a = 2^m - 1$.

Lemma 2.4 *Sei C ein Simplex-Code und $n = 2^m - 1$, dann hat $C^\perp$ Minimalgewicht größer gleich 2 genau dann, wenn $d = \frac{n+1}{2} (= 2^{m-1})$.*

BEWEIS Da C ein Simplex-Code ist, gilt nach der MacWilliams-Identität (siehe Vortrag „Gewichtszähler von Codes“) für den Dualcode von C

$$\begin{aligned} W_{C^\perp} &= \frac{1}{2^m} W_C(X+Y, X-Y) \\ &= \frac{1}{2^m}\left((X+Y)^n + a(X+Y)^{n-d}(X-Y)^d\right). \end{aligned}$$

Der Dualcode hat genau dann Gewicht größer 2, wenn der Koeffizient von $X^{n-1}Y$ im Gewichtszähler 0 ist. Durch Auflösen mit Hilfe des Binomischen Lehrsatzes erhält man für den Koeffizienten

$$\frac{1}{2^m}(n + n(n-d-d)) = \frac{1}{2^m} n(n+1-2d).$$

Der Koeffizient ist nun genau dann 0, wenn $d = 2^{m-1}$. ∎

2.1 Der verallgemeinerte Hamming-Code

Jetzt wollen wir den Nutzen der gezeigten Sätze verdeutlichen, indem wir den zu Beginn des Kapitels vorgestellten Hamming-Code auf höhere Dimensionen verallgemeinern. Sei dazu $p = 2$, $q = 2^m$ und $n = q-1 = 2^m - 1$. Sei α eine primitive n-te Einheitswurzel, also ein Erzeuger der Einheitengruppe, und $g(x) := \mu_\alpha \in \mathbb{F}_2[X]$ das Minimalpolynom von α. Nach den Anmerkungen am Anfang ist das Polynom $g(x)$ das Produkt der Linearfaktoren aus der Bahn der Operation der Galois-Gruppe vom Element α. Damit ist das Polynom gegeben durch

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)\cdots(x-\alpha^{2^{m-1}}).$$

Der von g erzeugte zyklische Code $C \subset \mathbb{F}_2^n$ heißt der verallgemeinerte Hamming-Code, ein BCH-Code mit geplantem Gewicht 2, Länge n und Dimension $n-m$.

Satz 2.5 *Der verallgemeinerte Hamming-Code C ist ein perfekter Code mit Minimalgewicht* 3.

BEWEIS Obwohl es sich bei C um einen BCH-Code mit geplantem Gewicht 2 handelt, folgt aus der Form des Erzeugerpolynoms $g(x)$ mit Satz (2.2) ein Minimalgewicht von mindestens 3. Ist C ein $[n,k,d]$-Code mit $d \geq 2t+1$, so sind die t-Hammingsphären $\{x \in \mathbb{F}_2^n \mid d(x,c) \leq t\}$ für $c \in C$ jeweils paarweise disjunkt. Zählt man die Wörter in $\mathbb{F}_2^n$ ab, die durch die Sphären überdeckt werden, so ergibt sich

$$2^{n-m}\left[1 + \binom{n}{1} + \cdots + \binom{n}{t}\right] \leq 2^n,$$

da genau 2^n Elemente in $\mathbb{F}_2^n$ existieren. Es muss aber $t \leq 1$ sein, da für $t = 1$ schon gilt

$$2^{n-m}\,[1+n] = 2^n.$$

Damit kann das Minimalgewicht aber nicht größer als $d = 4$ sein.

Angenommen das Minimalgewicht ist 4, so muss ein Codewort $c(x) \in C$ mit diesem Gewicht existieren. Sei $x \in \mathbb{F}_2^n$ von Gewicht 2 mit $d(x, c) = 2$. Da die 1-Hammingsphären der Codewörter den ganzen Raum überdecken, existiert weiter ein Codewort $c' \in C$ mit $d(c', x) = 1$. Da der Hammingabstand eine Metrik ist, folgt $d(c', c) \leq d(c, x) + d(x, c') = 3$, was im Widerspruch zur Voraussetzung steht. Also hat C Minimalgewicht 3 und ist damit ein perfekter Code nach der Definition aus dem Vortrag „Golay-Code und Leech-Gitter“. ∎

Der verallgemeinerte Hamming-Code ist also für $n = 2^m - 1$ ein $[n, n-3, 3]$-Code über dem $\mathbb{F}_2$. Durch die gewählte Konstruktion können wir jetzt leicht den Dualcode konstruieren, der eine besondere Gestalt hat.

Satz 2.6 *Der Dualcode $C^\perp$ des Hamming-Codes ist ein Simplexcode mit Minimalgewicht 2^{m-1}.*

Beweis Der Dualcode $C^\perp$ ist nach Voraussetzung ein linearer Code der Länge n und Dimension m. Da $C^\perp$ ein Code über dem $\mathbb{F}_2$ ist, hat er genau $2^m = n + 1$ Codewörter. Nach Lemma (2.3) wird der Code erzeugt von $\tilde{h}$ mit $\deg(\tilde{h}) = n - m$. Also sind die Wörter

$$0, \tilde{h}, x\tilde{h}, \ldots, x^{n-1}\tilde{h}$$

jeweils Elemente des Codes. Wir zeigen, dass sie alle verschieden sind. Angenommen es existieren $r, s \in \{0, \ldots, n-1\}$ mit $r \neq s$ und $x^s\tilde{h} = x^r\tilde{h}$. Dann folgt, dass $(x^r - x^s)\tilde{h}$ von $x^n - 1$ geteilt werden muss. Dann gilt aber insbesondere für jede n-te Einheitswurzel β in $\mathbb{F}_q^n$, dass $(\beta^r - \beta^s)\tilde{h}(\beta) = 0$ ist. Insbesondere ist α^{-1} eine n-te Einheitswurzel und $h(\alpha) \neq 0$. Also gilt nach Konstruktion auch $\tilde{h}(\alpha^{-1}) \neq 0$ und damit

$$\alpha^{-r} - \alpha^{-s} = 0.$$

Da α^{-1} genau wie α eine primitive n-te Einheitswurzel ist, ist dies nicht möglich.

Also wurden auf obige Weise alle Codewörter konstruiert, sie liegen dabei alle im Zykel des Erzeugerpolynoms. Damit haben sie alle dasselbe Gewicht und $C^\perp$ ist ein Simplex-Code, dessen Minimalgewicht nach Lemma (2.4) 2^{m-1} beträgt. ∎

3 Quadratische Restcodes

Quadratische Restcodes (QR-Codes) sind eine besondere Klasse von zyklischen Codes über dem $\mathbb{F}_2$, die analog zu den BCH-Codes über Polynome in Erweiterungskörper konstruiert werden. Die Idee ist dabei, das Erzeugerpolynom durch quadratische Reste in Primzahlkörpern zu konstruieren.

Definition 3.1 *Sei $p \in \mathbb{N}$ prim. Dann heißt ein Element $r \in \mathbb{F}_p \setminus \{0\}$ ein quadratischer Rest modulo p, wenn ein $a \in \mathbb{F}_p$ existiert mit*

$$r = a^2.$$

Ein Element, welches kein quadratischer Rest ist, heißt auch quadratischer Nichtrest. Der Körper lässt sich disjunkt in die quadratischen Reste, Nichtreste und die 0 zerlegen.

Satz 3.2 *Sei $p \in \mathbb{N}$ prim, $p > 2$. Für die Zerlegung*

$$\mathbb{F}_p = \{0\} \dot\cup Q \dot\cup N,$$

wobei Q die Menge der quadratische Reste und N die Menge der Nichtreste ist, gilt

$$|Q| = |N| = \frac{p-1}{2}.$$

Die Menge der quadratischen Reste Q ist eine Untergruppe von $\mathbb{F}_p^*$ und N ist die nichttriviale Nebenklassen von Q.

Beweis Jeder quadratische Rest $q = a^2 \pmod p$ hat mindestens zwei Quadratwurzeln a und $-a$, welche verschieden sind, da $p \neq 2$. Weiter hat jedoch das Polynom $h = x^2 - a$ maximal zwei Wurzeln, also hat q genau zwei Quadratwurzeln. Damit hat jedes Urbild der Abbildung

$$f : \mathbb{F}_p^* \to Q, x \mapsto x^2 \pmod p$$

genau zwei Elemente und somit die Menge der quadratischen Reste $\frac{n-1}{2}$ Elemente, da f surjektiv ist.

Die Menge der quadratischen Reste ist unter Multiplikation abgeschlossen, da für $r_1 = a_1^2 \in \mathbb{F}_p$ und $r_2 = a_2^2 \in \mathbb{F}_p$ auch $r_1 r_2 = (a_1 a_2)^2$ ein quadratischer Rest ist. Also ist Q eine Untergruppe von $\mathbb{F}_p^*$ von Index 2. Es existiert nur eine nichttriviale Nebenklasse, diese ist durch die Menge N der Nichtreste gegeben. ∎

Aus der Gruppenstruktur folgen einige Regeln für die Multiplikation von quadratischen Resten und Nichtresten.

Korollar 3.3 *Seien $r, s \in Q$ und $n, m \in N$. Dann gilt $rs \in Q, nm \in Q$ und $rn \in N$.*

Wir wollen nun die QR-Codes definieren. Dazu muss man für die Primzahl p zusätzlich

$$p \equiv 7 \pmod 8$$

fordern. Wählt man m mit $2^m - 1 \equiv 0 \pmod p$, so hat die Einheitengruppe $\mathbb{F}_{2^m}^*$ die Ordnung $2^m - 1$ und damit eine Teilgruppe der Ordnung p, welche insbesondere p verschiedene Wurzeln von $x^p - 1$ enthält. Wir setzen $m := p - 1$. Also zerfällt das Polynom $x^p - 1$ über $\mathbb{F}_{2^m}$ in Linearfaktoren. Der Erzeuger einer solchen Teilgruppe der Ordnung p ist eine primitive p-te Einheitswurzel α und damit zerfällt das Polynom in

$$x^p - 1 = \prod_{j=0}^{p-1} (x - \alpha^j).$$

Man kann weiter $x^p - 1$ in die α-Potenzen zu quadratischen Resten und zu Nichtresten zerlegen. Da α eine p-te Einheitswurzel ist, ist das Potenzieren mit Elementen aus $\mathbb{F}_p$ durch einen Vertreter wohldefiniert, zur Vereinfachung der Notation identifizieren wir die Elemente aus $\mathbb{F}_p$ mit ihren Vertretern $\{0, \ldots, p-1\} \subset \mathbb{Z}$.

Definition 3.4 *Sei*

$$g(x) := \prod_{r \in Q} (x - \alpha^r), \quad h(x) := \prod_{r \in N} (x - \alpha^r),$$

*dann gilt $g(x)h(x)(x-1) = x^p - 1$ und man nennt den von $g(x)$ erzeugten zyklischen Code C einen **quadratischen Restcode** zur Primzahl p.*

Wie auch schon bei BCH-Codes wollen wir diesen Code auch über dem $\mathbb{F}_2$ betrachten können. Hierzu benötigen wir die bisher unmotivierte Bedingung $p \equiv 7 \pmod 8$. Ohne Beweis zitieren wir aus [4] folgendes Lemma.

Lemma 3.5 *Sei p eine Primzahl mit $p \equiv 7 \pmod 8$. Dann ist 2 ein quadratischer Rest und -1 ein quadratischer Nichtrest in $\mathbb{F}_p$. Mit Korollar (3.3) gilt insbesondere $2Q = Q$ und $-Q = N$.*

Damit erhalten wir wie gewünscht den folgenden Satz.

Satz 3.6 *Die Polynome $g(x)$ und $h(x)$ haben Koeffizienten in $\mathbb{F}_2$.*

BEWEIS Die Elemente aus $\mathbb{F}_2 \subset \mathbb{F}_{2^m}$ sind genau die Idempotenten des Körpers $\mathbb{F}_{2^m}$. Also reicht es, für jeden Koeffizienten a des Polynoms die Identität $a^2 = a$ zu zeigen.

Da $g(x)$ gegeben ist durch $g(x) = \prod_{r \in Q}(x - \alpha^r)$, erhalten wir den Koeffizienten zur Potenz i, $0 \leq i \leq |Q|$ als die Summe

$$\text{Koeff}_i(g(x)) = \sum_{M \in \text{Pot}_i(Q)} \left(\prod_{k \in Q - M} \alpha^k \right).$$

Da $\mathbb{F}_{2^m}$ Charakteristik 2 hat, folgt für das Quadrat

$$\text{Koeff}_i(g(x))^2 = \left(\sum_{M \in \text{Pot}_i(Q)} \prod_{k \in Q - M} \alpha^k \right)^2 = \sum_{M \in \text{Pot}_i(Q)} \prod_{k \in Q - M} \alpha^{2k}.$$

Es bleibt also zu zeigen, dass gilt

$$\prod_{r \in Q}(x - \alpha^{2r}) = \prod_{r \in Q}(x - \alpha^r).$$

Da aber nach Lemma (3.5) 2 ein quadratischer Rest in $\mathbb{F}_p$ ist, ist die Menge Q abgeschlossen unter Multiplikation mit 2. Also folgt die Gleichheit der obigen Terme und damit auch die Aussage für $g(x)$. Das Polynom $h(x)$ erhält man durch die Polynomdivision von $x^p - 1$ mit $g(x)(x - 1)$, es hat also Koeffizienten in $\mathbb{F}_2$. ∎

Also ist der QR-Code C ein binärer Code der Dimension $\frac{p+1}{2}$. Offensichtlich hängt die Konstruktion des Codes von der gewählten Einheitswurzel α ab. Da -1 kein quadratischer Rest ist, kann man beispielsweise α^{-1} zu Konstruktion benutzen und erhält einen anderen Code. Es stellt sich also die Frage, wie viele QR-Codes zu gegebener Primzahl p existieren.

Lemma 3.7 *Es gibt genau zwei QR-Codes zur Primzahl p.*

BEWEIS Die Menge der p-ten Einheitswurzeln ist eine zyklische Teilgruppe von $\mathbb{F}_{2^m}$ der Ordnung p. Da p eine Primzahl ist, ist insbesondere jedes Element außer der Eins ein Erzeuger. Also hat für eine beliebige primitive p-te Einheitswurzel $\beta \in \mathbb{F}_{2^m}$ die Menge der Potenzen von β zu quadratischen Resten die Form

$$\{\beta^i \mid i \in Q\} = \begin{cases} \{\alpha^i \mid i \in Q\}, & \text{für } \alpha \in \{\beta^i \mid i \in Q\} \\ \{\alpha^i \mid i \in -Q = N\}, & \text{für } \alpha \in \{\beta^i \mid i \in N\} \end{cases}.$$

Daher gibt es genau zwei verschiedene QR-Codes. Zu gegebener primitiver p-ter Einheitswurzel ensteht der zweite Code durch Substitution von $\alpha \mapsto \alpha^{-1}$. ∎

Aufgrund der gleichen Dimension ist klar, dass beide Codes isomorph als Vektorräume sind. Von Interesse in diesem Vortrag ist jedoch die Struktur des Codes als Code. Doch auch hier erhalten wir Äquivalenz.

Satz 3.8 *Bis auf Äquivalenz existiert nur ein QR-Code zur Primzahl p.*

BEWEIS Sei C der von $g(x)$ erzeugte QR-Code und $\hat{C}$ der zweite, von $h(x)$ erzeugte Code. Nach Lemma (3.5) ist -1 ein quadratischer Nichtrest. Wir betrachten das Polynom

$$q(x) := g(x^{-1}) = \prod_{i \in Q} (x^{-1} - \alpha^i).$$

Für die primitive p-te Einheitswurzel α gilt $\alpha^i = (\alpha^{-i})^{-1}$, insbesondere ist α^{-i} eine Wurzel von $q(x)$ für jedes $i \in Q$. Da $-Q = N$, folgt $h(x)$ teilt $q(x)$. Also schickt die $\mathbb{F}_2$-lineare Abbildung $\varphi \colon \mathbb{F}_2[x]/\langle x^p - 1\rangle \to \mathbb{F}_2[x]/\langle x^p - 1\rangle$ gegeben durch $x^i \mapsto x^{-i}$ für $1 \leq i \leq p-1$ jedes Codewort des QR-Codes C auf ein Wort des zweiten QR-Codes $\hat{C}$.

Die Abbildung φ ist bijektiv, denn φ schickt die Basis $(1, x, \ldots, x^{p-1})$ auf eine Permutation von sich. Aus Dimensionsgründen ist damit auch die Einschränkung $\varphi : C \to \hat{C}$ bijektiv. Durch φ werden die Koordinaten des Codes permutiert, also definiert die Abbildung die Permutation

$$\sigma := \begin{pmatrix} 0 & 1 & 2 & \ldots & p-1 \\ 0 & \overline{1} & \overline{2} & \ldots & \overline{p-1} \end{pmatrix},$$

mit $\overline{i}$ dem Vertreter aus $\{0, \ldots, p-1\}$ von $-i \in \mathbb{F}_p$. Damit ist $\hat{C} = \sigma(C)$ und es folgt die Äquivalenz der Codes. ∎

Dies erleichtert den Umgang mit QR-Codes, da es die Bezeichnung des Codes als den QR-Code zur Primzahl p rechtfertigt. Im weiteren werden wir meist darauf verzichten, Fälle bezüglich der Codes zu unterscheiden. Jetzt wollen wir uns den strukturellen Eigenschaften dieser Konstruktion zuwenden. Dazu betrachten wir zunächst das Gewicht von Codewörtern.

Satz 3.9 *Sei $a \in C$ ein Codewort mit Gewicht $w(a) = d$.*

(i) Ist d ungerade, so gilt $d^2 - d + 1 \geq p$ sowie $d \equiv 3 \pmod 4$.

(ii) Ist d gerade, so gilt $d \equiv 0 \pmod 4$.

BEWEIS Wegen $w(a) = d$ existieren paarweise verschiedene $k_i \in \{0, \ldots, p-1\}$ mit $1 \leq i \leq d$, sodass $a(x) = \sum_{i=1}^{d} x^{k_i}$. Setze $\hat{a}(x) := a(x^{-1})$. Dann gilt $a(\alpha^r) = 0$ für $r \in Q$ und $\hat{a}(\alpha^n) = 0$ für $n \in N$.

Sei d ungerade. Dann ist $a(1) \neq 0 \neq \hat{a}(1)$ und $a(r)\hat{a}(r) = 0$ für alle $r \in N \cup Q$. Mit der Faktorisierung $x^p - 1 = (x-1)(1 + x + \cdots + x^{p-1})$ folgt $a(x)\hat{a}(x)$ teilt $1 + x + \cdots + x^{p-1}$ und

damit folgt Gleichheit in $\mathbb{F}_2[x]/\langle x^p-1\rangle$. Das Gewicht von $a(x)\hat{a}(x)$ ist gleich der Anzahl an Monomen p. Offensichtlich hat $a(x)\hat{a}(x)$ maximal d^2 Koeffizienten ungleich 0. Beim Ausmultiplizieren fallen jedoch einige Terme zusammen. Von den d^2 Monomen fallen d Stück der Form $x^{k_i}x^{-k_i}$ zusammen zu einem Koeffizienten der Potenz 0. Da d ungerade ist, erhält man eine 1 als Koeffizient und es muss also gelten, dass $d^2-d+1 \geq p$ ist.

Die weitere Möglichkeit, durch die sich Koeffizienten auslöschen können, ist bei Gleichheit von zwei Monomen $x^{k_i}x^{-k_j} = x^{k_n}x^{-k_m}$. Dann existiert aber immer das weitere Paar $x^{-k_i}x^{k_j} = x^{-k_n}x^{k_m}$. Es löschen sich also gleich 4 Terme aus. Also existiert ein $e \in \mathbb{N}_0$, sodass $d^2-d+1-4e = p$ gilt. Da d ungerade ist, folgt mit $p \equiv 7 \pmod 8$ schon $d \equiv 3 \pmod 4$.

Sei nun d gerade. Es folgt, dass $a(1)\hat{a}(1) = 0$ und entsprechend $a(x)\hat{a}(x) = x^p - 1$ in $\mathbb{F}_2[x]/\langle x^p-1\rangle$. Also ist $w(a(x)\hat{a}(x)) = 0$ und mit analoger Argumentation zu Fall d ungerade erhält man $d^2-d-4e = 0$ und damit $d \equiv 0 \pmod 4$. ∎

Es ist noch nicht klar, ob ein QR-Code gerades oder ungerades Minimalgewicht hat. Daher lassen sich bis jetzt noch keine genaueren Aussagen über das Minimalgewicht treffen. Von dem erweiterten QR-Code $\tilde{C} \subset \mathbb{F}_2^{p+1}$ weiß man jedoch Entsprechendes.

Korollar 3.10 *Der erweiterte QR-Code $\tilde{C}$ ist doppelt gerade und selbstdual.*

Beweis Der Code $\tilde{C}$ ist doppelt gerade nach (3.9) und damit gilt $\tilde{C} \subset \tilde{C}^\perp$. Da

$$\dim \tilde{C} = \dim C = p - \frac{p-1}{2} = \frac{p+1}{2},$$

folgt $\tilde{C} = \tilde{C}^\perp$ aus Dimensionsgründen. ∎

Wir wollen nun die Automorphismengruppe des erweiterten QR-Codes genauer betrachten. Dafür benötigen wir ein Erzeugendensystem des Codes. In (1.4) hatten wir bereits gesehen, dass jeder zyklische Code, und damit insbesondere der QR-Code, einen idempotenten Erzeuger hat.

Lemma 3.11 *Das Polynom $c(x) := \sum_{r\in Q} x^r \in \mathbb{F}_2[x]$ oder $c'(x) := \sum_{n\in N} x^n \in \mathbb{F}_2[x]$ ist das erzeugende Idempotent des QR-Codes C.*

Beweis Analog zum Vorgehen in Satz (3.6) erhalten wir

$$c(x)^2 = \sum_{r\in Q} x^{2r} \equiv \sum_{r\in Q} x^r = c(x) \pmod{x^p-1}.$$

Entsprechendes gilt für $c'(x)$. Also handelt es sich um Idempotenten, falls es Codewörter sind, das heißt falls $c(\alpha^s) = 0$ bzw. $c'(\alpha^s) = 0$ für alle $s \in Q$ und diese Wörter eine Eins

des Codes bilden. Dazu betrachten wir p-te Einheitswurzeln β. Aus der Idempotenz folgt $c(\beta), c'(\beta) \in \{0,1\}$ und nach Voraussetzung $c(1) = c'(1) = \frac{p-1}{2} = 1$ in $\mathbb{F}_2$, da $p \equiv 7 \pmod 8$ und somit $\frac{p-1}{2} \equiv 3 \pmod 4$.

Für $\beta \neq 1$ gilt dann

$$1 = \sum_{r \in Q \cup N} \beta^r = c(\beta) + c'(\beta),$$

da nach Voraussetzung $\sum_{r=0}^{p-1} \beta^r = g(r)h(r) = 0$ gilt und damit $\sum_{r \in Q \cup N} \beta^r = 0 - 1 = 1$ ist. Weiter gilt $c(\alpha^s) = c(\alpha), c'(\alpha^s) = c'(\alpha)$ für alle $s \in Q$, da die Menge der quadratischen Reste und Nichtreste unter Multiplikation mit quadratischen Resten abgeschlossen ist.

Da aber $c(\alpha) + c'(\alpha) = 1$ ist, schickt insbesondere genau eines der Polynome jede α-Potenz auf 0 und liegt damit im Code. Dieses Element liefert das gesuchte Idempotent. Das verbleibende Polynom ist dann genau das Idempotent für den durch α^{-1} erzeugten äquivalenten QR-Code.

Noch zu zeigen ist, dass dieses Idempotent auch eine Identität des Codes ist. Dazu sei nun ohne Einschränkung $c(x)$ das Idempotent des Codes. Wie oben gezeigt wurde, ist $g(x)$ ein Teiler von $c(x)$. Es gilt weiter $h(x)$ teilt $1 - c(x)$, da für jede Wurzel α von $h(x)$ gilt, dass α eine p-te Einheitswurzel ungleich 1 ist, also insbesondere $c(x) = 1$ gilt. Daraus folgt aber $1 - c(x) = 0$ und damit die gewünschte Beziehung.

Es existiert aber in Analogie zum Beweise von Satz (1.4) eine Darstellung der Eins $1 = c(x) + b(x)h(x)$, damit also $c(x) = 1 - b(x)h(x)$ und $c(x)$ ist eine Identität des Codes. ∎

Dieses Codewort kann man nun nutzen, um eine Erzeugendenmatrix des Codes anzugeben. Sei $c(x) = c_0 + c_1 x + \cdots + c_{p-1}x^{p-1}$ der idempotente Erzeuger von C. Nach der Definition gilt also $c_r = 1$, falls $r \in Q$ und $c_r = 0$, falls $r \notin Q$. Aus $p \equiv 7 \pmod 8$ folgt, dass $\frac{p-1}{2}$ ungerade ist, also ist das Paritätsbit für $c(x)$ gleich 1. Weiterhin ist der erweiterte Code doppelt gerade und selbstdual, enthält also das konstante 1 Wort, da dieses im Skalarprodukt über $\mathbb{F}_2$ mit jedem geraden Codewort 0 ergibt. Schreibt man dieses Wort nach oben, so erhält man folgende Matrix

$$G := \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & c_0 & c_1 & \dots & c_{p-1} \\ 1 & c_{p-1} & c_0 & \dots & c_{p-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & c_1 & c_2 & \dots & c_0 \end{pmatrix},$$

die den Code erzeugt. Wir identifizieren die Koordinaten in $\mathbb{F}_2^{p+1}$ mit den Elementen der projektiven Ebene $\mathbb{P}_1(\mathbb{F}_p) = \{\infty, 0, 1, \dots, p-1\}$ in gegebener Reihenfolge. Dann operiert

die Gruppe $\mathrm{PSL}_2(\mathbb{F}_p)$ auf den Koordinaten durch gebrochen lineare Transformation $z \mapsto \frac{az+b}{cz+d}$. Die Operation ist doppelt transitiv, da jedes Paar von verschiedenen Elementen auf $(0, \infty)$ gebracht werden kann.

Satz 3.12 *Für die Automorphismengruppe des erweiterten QR-Codes $\tilde{C}$ gilt*

$$\mathrm{PSL}_2(\mathbb{F}_p) \subset \mathrm{Aut}(\tilde{C}).$$

BEWEIS Nach dem Vortrag „Modulformen“ ist die $\mathrm{PSL}_2(\mathbb{F}_p)$ erzeugt durch die Transformationen $T : z \mapsto z + 1$ und $S : z \mapsto -\frac{1}{z}$.

Betrachen wir zunächst T. Es ist T eine zyklische Transformation, die das Paritätsbit an der Position ∞ fest lässt. Also liegt insbesondere die Transformation jedes Codewortes wieder im Code, da es sich um einen zyklischen Code handelt.

Es bleibt zu zeigen, dass auch S in den Code abbildet. Dazu nummerieren wir auch die Zeilen der Matrix mit $\{\infty, 0, 1, \ldots, p-1\}$ durch. Damit erhält man $G = (g_{i,j})_{i,j \in \mathbb{P}_1(\mathbb{F}_p)}$ und definiert

$$h_{i,j} := S g_{i,j} = g_{-1/i, -1/j}, H := (h_{i,j}).$$

Es ist also zu zeigen, dass die Zeilen in H wieder Elemente des Codes sind. Dazu betrachten wir die verschiedenen Fälle, die für $i \in \mathbb{P}_1(\mathbb{F}_p)$ auftreten können.

1. Fall $i = 0$:
Da S nach Definition 0 und ∞ austauscht, folgt $h_{0,j} = g_{\infty, -1/j} = 1$, da in der ersten Zeile der Erzeugermatrix G nur 1-en stehen. Also erhält man insbesondere eine Zeile aus G und damit ein Wort aus C.

2. Fall $i = \infty$:
Es gilt, dass S einen quadratischen Rest auf einen quadratischen Nichtrest schickt (und umgekehrt), da die quadratischen Reste unter Multiplikation mit quadratischen Resten abgeschlossen sind, aber $j \cdot -\frac{1}{j} = -1 \notin Q$ gilt. Da in der Zeile 0 genau das Codewort $c(x)$ steht, gilt $g_{0,j} = 0$ falls $j \in N$ und $g_{0,j} = 1$ falls $j \in Q$. Damit folgt

$$h_{\infty,j} = \begin{cases} g_{0,-\frac{1}{j}} = 1 + g_{0,j} = g_{\infty,j} + g_{0,j}, & \text{für } j \in \{1, 2, \ldots, p-1, \infty\} \\ g_{0,\infty} = 1 = g_{\infty,j} + g_{0,j}, & \text{für } j = 0 \end{cases},$$

also die Summe von zwei Spalten aus G und damit ein Codewort.

3. Fall $i \in Q$:
Wir betrachten die Summe der i-ten Zeilen von G und H. Nach der Konstruktion von G gilt $g_{i,j} = g_{0,j-i}$, da die i-te Zeile genau die i-fach verschobene Zeile ist. Es folgt, dass $h_{i,j} = g_{0,-1/j+1/i}$. Also ist $g_{i,j} + h_{i,j}$ gleich 0, falls $j = i$ oder $j = \infty$ und 1 für $j = 0$. Ist $j \in N$, so ist $j - i \in Q$ genau dann, wenn $\frac{j-i}{ij} \in N$, da $(ij)^{-1} \in N$. Wir erhalten also

$g_{i,j} + h_{i,j} = 1$. Ebenso erhalten wir für $j \in Q$ mit $j \neq i$, dass $j - i \in Q$ genau dann, wenn $\frac{j-i}{ji} \in Q$ und damit $g_{i,j} + h_{i,j} = 0$.

Insgesamt ergibt sich die Summe von i-ten Zeilen von G und H als die Summe der Zeilen 0 und ∞ von G. Damit ist die i-te Zeile von H genau die Summe der Zeilen $\infty, 0$ und i von G, also insbesondere Element des Codes.

4. Fall $i \in N$:
Analog zum 3. Fall betrachten wir die Summe der i-ten Zeilen. Wir erhalten $g_{i,j} + h_{i,j}$ gleich 1 für $j = \infty$ sowie 0 für $j = 0$ und $j = i$. Für $j \in N$ mit $j \neq i$ ist $j - i \in Q$ genau dann, wenn $\frac{j-i}{ij} \in Q$. In diesem Fall erhalten wir $g_{i,j} + h_{i,j} = 0$. Für $j \in Q$ ist $j - i \in Q$ genau dann, wenn $\frac{j-i}{ij} \in N$ und wir erhalten $g_{i,j} + h_{i,j} = 1$. Damit ist die i-te Zeile von H genau die Summe der 0-ten und der i-ten Zeile von G und damit Element des Codes. ∎

Also operiert die Automorphismengruppe des erweiterten QR-Codes als Obergruppe der $\mathrm{PSL}_2(\mathbb{F}_p)$ transitiv auf den Positionen der Codewörter. Nun können wir die in (3.9) gezeigten Abschätzungen auf den Code anwenden.

Korollar 3.13 *Das Minimalgewicht eines QR-Codes ist ungerade. Damit gilt für jeden QR-Code C zur Primzahl p*

(i) $d(C) \equiv 3 \pmod 4$,

(ii) $d(C)^2 - d(C) + 1 \geq p$,

(iii) $d(\tilde{C}) = d(C) + 1$.

Beweis Sei $\tilde{a}(x)$ ein Wort minimalen Gewichts in $\tilde{C}$. Da die $\mathrm{PSL}_2(\mathbb{F}_p)$ transitiv auf den Positionen operiert kann man ohne Einschränkungen davon ausgehen, dass $\tilde{a}(x)$ eine 1 an der Stelle des Paritätsbits hat. Durch Entfernen des Paritätsbits erhält man ein Codewort $a(x) \in C$ mit $w(a(x)) = w(\tilde{a}(x)) - 1$. Da $\tilde{C}$ doppelt gerade ist, folgt, dass $w(a(x))$ ungerade ist. Die restlichen Abschätzungen folgen sofort aus (3.9). ∎

Zum Abschluss des Abschnitts wollen wir noch zwei bekannte Beispiele für quadratische Restcodes betrachten, die auch schon in vorherigen Vorträgen behandelt wurden.

Beispiel 3.14 *Wir betrachten den QR-Code C zu $p = 7$. Es ergibt sich Minimalgewicht ≥ 3 und Dimension $\frac{7+1}{2} = 4$. Wir erhalten also eine weitere Konstruktion des Hamming-Codes. Nach dem Vortrag „Codes und Codegitter“ hat der Hamming-Code als Automorphismengruppe die $\mathrm{GL}_3(\mathbb{F}_2)$.*

Man erhält die Automorphismengruppe des Hamming-Codes als Stabilisator des Paritätsbits in der Automorphismengruppe des erweiterten Hamming-Codes. Da $\mathrm{Aut}(\tilde{C})$ transitiv

auf den Koordinaten operiert, existieren weitere Elemente, die das Paritätsbit nicht fest lassen und es folgt

$$|\operatorname{Aut}(\tilde{C})| > |\operatorname{GL}_3(\mathbb{F}_2)| = 168 = |\operatorname{PSL}_2(\mathbb{F}_7)|.$$

Der Hamming-Code ist also ein Beispiel, in dem die echte Teilmengenbeziehung aus Satz (3.12) gilt.

Für $p = 23$ erhalten wir den aus dem Vortrag „Golay-Code und Leech-Gitter“ bekannten Golay-Code.

Beispiel 3.15 *Sei C der QR-Code zur Primzahl $p = 23$. Dann ist C ein $[23, 12]$-Code. Da $5^2 - 5 + 1 = 21 < 23$, erhalten wir $d > 5$ und weiter $d \geq 7$ mit Korollar (3.13). Angenommen das Gewicht wäre größer 10. Dann existiert eine Erzeugermatrix des Codes $(I_{12} \mid A)$ mit $A \in \mathbb{F}_2^{12\times 11}$. Jede Zeile von A muss mindestens 10 Einsen enthalten, man erhält aber durch Linearkombinationen von Zeilen Wörter mit Gewicht kleiner 10, was einen Widerspruch liefert.*

Also ist C der eindeutige $[23, 12, 7]$-Golay-Code nach dem Vortrag „Golay-Code und Leech-Gitter“.

Literatur

[1] R.E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, 2003

[2] W. Ebeling, *Lattices and Codes*, Springer Fachmedien Wiesbaden, 2012

[3] L.R. Vermani, *Elements of Algebraic Coding Theory*, CRC Press, 1996

[4] E. Zerz, *Elementare Zahlentheorie*, 2011