Endliche Körper und Codierung

Manfred Madritsch

Institut für Mathematik A
Technische Universität Graz

Version: SS 2010

Achtung:
Bitte Anregungen und Fehler per Email an die Adresse `madritsch@tugraz.at` senden.

Dieses Skriptum wurde von Manfred Madritsch verfasst und basiert auf einer Mitschrift von Florian Lehner und Jan Pöschko.

Inhaltsverzeichnis

Kapitel 1

Endliche Körper

In diesem Skriptum bezeichnet p immer eine Primzahl und $q = p^n$ immer eine Primzahlpotenz mit Basis p und Exponent n.

1.1 Einleitung

Wir wollen uns zuerst erinnern, was wir unter einem Körper und im speziellen unter einem endlichen Körper verstehen. Dazu benötigen wir zuerst die einfachste algebraische Struktur, nämlich die der Gruppe.

Definition. Eine *multiplikative Gruppe* $(G, \cdot)$ ist eine Menge G auf welcher eine binäre Operation $\cdot : G \times G \to G$ derart definiert ist, dass

- $\forall a \in G, \forall b \in G : a \cdot b \in G$ (Abgeschlossenheit),
- $\forall a \in G, \forall b \in G, \forall c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativität),
- $\exists e \in G, \forall a \in G : a \cdot e = e \cdot a = a$ (dieses e ist eindeutig),
- $\forall a \in G, \exists b \in G : a \cdot b = b \cdot a = e$ (wir nennen b das Inverse von a und schreiben kurz a^{-1}).

Gilt darüber hinaus, dass

$$\forall a \in G, \forall b \in G : ab = ba,$$

dann nennt man die Gruppe *abelsch oder kommutativ.*

Wir werden uns nicht nur mit Gruppen aufhalten sondern wollen noch eine zweite Operation hinzunehmen und Ringe definieren.

Definition. Ein Tripel $(R, +, \cdot)$ heißt Ring, wenn

- $(R, +)$ eine Gruppe ist,
- $\forall a \in G, \forall b \in G, \forall c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativität),
- $\forall a \in G, \forall b \in G, \forall c \in G : a \cdot (b + c) = a \cdot b + a \cdot c \wedge (a + b) \cdot c = a \cdot c + b \cdot c.$

Gilt darüber hinaus, dass

$$\forall a \in R, \forall b \in R : ab = ba,$$

dann nennt man den Ring *kommutativ.*

Wir werden immer mit 0 das neutrale Element der Addition und mit 1 das der Multiplikation bezeichnen. Mit diesen beiden Strukturen im Gepäck können wir ganz leicht einen Körper definieren.

Definition. Ein Tripel $(K, +, \cdot)$ heißt Körper, wenn $(R, +, \cdot)$ ein Ring ist und $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist.

Zu guter Letzt benötigen wir noch die Definition eines Vektorraumes.

Definition. Ein Tripel $(V, +, K)$ heißt Vektorraum über K, wenn

- $(V, +)$ eine Abel'sche Gruppe ist,
- K ein Körper ist,
- es eine Skalar-Multiplikation $\times : K \times V \to V$ gibt, sodass
  - $\forall a \in V : 1 \times a = a$,
  - $\forall \alpha \in K, \forall \beta \in K, \forall a \in V : \alpha \times (\beta \times a) = (\alpha \cdot \beta) \times a$,
  - $\forall \alpha \in K, \forall a \in V, \forall b \in V : \alpha \times (a + b) = \alpha \times a + \alpha \times b$,
  - $\forall \alpha \in K, \forall \beta \in K, \forall a \in V : (\alpha + \beta) \times a = \alpha \times a + \beta \times a$.

Ein endlicher Körper ist nun ein Körper mit endlich vielen Elementen. Wir wissen:

- Wenn F ein Körper ist, dann ist die Kardinalität von F eine Primzahlpotenz.
- Zu jeder Primzahlpotenz $q = p^n$ gibt es einen Körper mit q Elementen.
- Je zwei Körper der gleichen endlichen Kardinalität sind isomorph. Wir sprechen damit von *dem* Körper mit p^n Elementen und schreiben dafür $\mathbb{F}_{p^n}$.
- Aufgrund des kleinen Satzes von Fermat gilt für alle $\beta \in \mathbb{F}_q \setminus \{0\}$, dass $\beta^{|\mathbb{F}_q \setminus \{0\}|} = \beta^{q-1} = 1$. Multiplikation mit β führt zu $\beta^q = \beta$. Diese Aussage gilt auch für $\beta = 0$. Also sind alle Elemente von $\mathbb{F}_q$ Nullstellen von $X^q - X$, der Körper $\mathbb{F}_q$ ist somit genau die Menge der Nullstellen von $X^q - X$.
- $\mathbb{F}_q$ ist der Zerfällungskörper von $X^q - X$ über $\mathbb{F}_p$. Mit dem Satz von Vieta folgt, dass

$$X^q - X = \prod_{\beta \in \mathbb{F}_q} (X - \beta).$$

Satz 1.1. *Die Abbildung $\Phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $x \mapsto x^p$ (Frobenius) ist ein Automorphismus von $\mathbb{F}_{p^n}$, der $\mathbb{F}_p$ fixiert.*

Beweis. Wir zeigen zuerst, dass Φ ein Homomorphismus ist. Dazu betrachten wir

$$\Phi(x + y) = (x + y)^p = \sum_{k=1}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = \Phi(x) + \Phi(y),$$
$$\Phi(x \cdot y) = (x \cdot y)^p = x^p y^p = \Phi(x) \cdot \Phi(y).$$

Nun betrachten wir den Kern der Abbildung und erhalten:

$$\Phi(x) = 0 \Leftrightarrow x^p = 0 \Leftrightarrow x = 0.$$

Damit folgt, dass $\mathrm{Ker}(\Phi) = \{0\}$ und somit ist Φ injektiv. Die Surjektivität folgt aus dem Vergleich der Kardinalitäten von Urbild und Bild. Damit ist Φ ein Automorphismus.
Es bleibt zu zeigen, dass Φ $\mathbb{F}_p$ fixiert. Es folgt aber mit dem kleinen Satz von Fermat, dass

$$\Phi(a) = a^p = a = \mathrm{id}(a) \quad \forall a \in \mathbb{F}_p.$$

□

Nachdem wir uns ein paar Eigenschaften in Erinnerung gerufen haben, wollen wir nun kanonische Beispiele für Endliche Körper geben. So ist für jede Primzahl p der Restklassenring $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ mit Addition und Multiplikation modulo p ein Körper. Für $q = p^n$ ist $\mathbb{F}_q = \mathbb{F}_p[X]/(f)$ für ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ vom Grad n.

Beispiel (Finde $\mathbb{F}_9$). Wir suchen ein irreduzibles Polynom vom Grad 2 über $\mathbb{F}_3$. Man sieht leicht, dass $f = X^2 + 1$ keine Nullstelle in $\mathbb{F}_3$ hat und daher irreduzibel ist (weil es ein Polynom vom Grad 2 ist). Also ist

$$\mathbb{F}_9 = \left\{a + b\alpha \mid a, b \in \mathbb{F}_3 \wedge \alpha^2 + 1 = 0\right\}$$

Um alle möglichen Polynome zu finden, betrachten wir die Faktorisierung von $X^9 - X$:

$$\begin{aligned} X^9 - X &= X(X^8 - 1) = X(X^4 - 1)(X^4 + 1) \\ &= X(X^2 - 1)(X^2 + 1)(X^4 + 1) \\ &= X(X - 1)(X + 1)(X^2 + 1)(X^2 + 2X + 2)(X^2 + X + 2). \end{aligned}$$

Damit erhalten wir, dass X^2+2X+2 und X^2+X+2 alternative Wahlen für das Minimalpolynom wären.
Nun berechnen wir beispielhaft $(1 + \alpha)(2 + \alpha)$ in $\mathbb{F}_9$ als

$$(1 + \alpha)(2 + \alpha) = 2 + 2\alpha + \alpha + \alpha^2 = 1 + (\alpha^2 + 1) = 1.$$

Wir haben nun die Inverse von $(1 + \alpha)$ gefunden.

Wie können wir in diesem Körper beliebige Inverse bezüglich der Multiplikation finden? Sei $g(\alpha) \in \mathbb{F}_q = \mathbb{F}_p[X]/(f)$, dann ist $g \in \mathbb{F}_p[X]$ ein Polynom mit $\deg g \leq n$. Falls $g(\alpha) \neq 0$ ist, ist f kein Teiler von g. $g \nmid f$ weil f irreduzibel ist.
Wir suchen ein multiplikatives Inverses zu g, also ein $h \in \mathbb{F}_p[X]$, das $g(\alpha)h(\alpha) = 1$ erfüllt. Das ist gleichbedeutend mit $g(X)h(X) = 1 + f(X)d(X)$ beziehungsweise $g(X)h(X) - f(X)d(X) = 1$.
Das ist lösbar, weil $\mathrm{ggT}(f, g) = 1$ ist. Die Lösung liefert der erweiterte euklidsche Algorithmus.

1.2 Zwischenkörperstruktur

Welche Körper gibt es zwischen $\mathbb{F}_p$ und $\mathbb{F}_{p^n}$? Kann es womöglich sein, dass es mehrere Zwischenkörper derselben Kardinalität gibt?

Lemma 1.2. *Sei $q = p^n$ eine Primzahlpotenz und K ein Teilkörper von $\mathbb{F}_q$. Dann gibt es ein $k \in \mathbb{N}$ mit $|K| = p^k$ und $k \mid n$.*

Beweis. $\mathbb{F}_q$ wird als K-Vektorraum gesehen. Setze $r := \dim_K \mathbb{F}_q$. Es ist also $\mathbb{F}_q$ als K-Vektorraum isomorph zu K^r. Somit gilt:

$$p^n = |\mathbb{F}_q| = |K^r| = |K|^r.$$

Aufgrund der eindutigen Primfaktprenzerlegung in $\mathbb{Z}$ muss $|K| = p^k$ für ein passendes k sein. Es gilt $p^n = p^{kr}$, also $n = kr$ beziehungsweise $k \mid n$. □

Satz 1.3 (Zwischenkörperstruktur)**.** *Sei $q = p^n$ und $k \in \mathbb{N}$ mit $k \mid n$. Dann gibt es genau einen Teilkörper von $\mathbb{F}_q$ der Kardinalität p^k.*

Beweis. Setze $r := p^k$. Alle Elemente eines solchen Teilkörpers sind Nullstellen von $X^r - X$. Also definieren wir $M := \{\alpha \in \mathbb{F}_q \mid \alpha^r = \alpha\}$. Zu zeigen sind folgende Aussagen:

- M ist ein Körper: Seien $\alpha, \beta \in M$, dann gilt

  $(\alpha+\beta)^r = \alpha^r + \beta^r = \alpha + \beta$ (laut Algebra-Übung)
  $(\alpha\beta)^r = \alpha^r\beta^r = \alpha\beta$
  $(-1)^r = -1$ (für ungerades r klar, bei gerader Charakteristik gibt es keine Vorzeichenfehler)
  $\left(\frac{1}{\alpha}\right)^r = \frac{1}{\alpha^r} = \frac{1}{\alpha}$ (für $\alpha \neq 0$)

- $|M| = r$:
  - $|M| \leq r$: Das Polynom $X^r - X$ hat höchstens r Nullstellen in $\mathbb{F}_q$.
  - $|M| = r$: Wir werden zeigen, dass $X^r - X$ über $\mathbb{F}_q$ in Linearfaktoren zerfällt.
    Es gilt $n = mk$, also ist

    $$\begin{aligned} q - 1 &= p^{mk} - 1 \\ &= r^m - 1 \\ &= (r-1)(r^{m-1} + r^{m-2} + \cdots + 1) \\ &=: (r-1)s. \end{aligned}$$

    Weiters gilt nun

    $$\begin{aligned} X^q - X &= X(X^{q-1} - 1) \\ &= X\left((X^{r-1})^s - 1\right) \\ &= X(X^{r-1} - 1)\left((X^{r-1})^{s-1} + \cdots + 1\right) \\ &= (X^r - X)\left((X^{r-1})^{s-1} + \cdots + 1\right). \end{aligned}$$

    Da $X^q - X$ über $\mathbb{F}_q$ in Linearfaktoren zerfällt, muss auch $X^r - X$ in Linearfaktoren zerfallen. Also hat $X^r - X$ genau r Nullstellen in $\mathbb{F}_q$.

- M ist der einzige mögliche Teilkörper dieser Kardinalität: Da alle Kandidaten für Körperelemente im Körper enthalten sein müssen, gibt es keine weitere Möglichkeit einen Körper dieser Kardinalität zu finden. □

Bemerkung. Wir haben $\mathbb{F}_q$ bisher als Körpererweiterung von $\mathbb{F}_p$ gesehen. Genau so gut kann $\mathbb{F}_q$ als Körpererweiterung von $\mathbb{F}_{p^k}$ gesehen werden $(k \mid n, q = p^n)$.
Wir denken daher oft an $\mathbb{F}_{q^n}$ als Körpererweiterung von $\mathbb{F}_q$.

1.3 Automorphismenstruktur

Wir denken an Polynome der Form $x^2 + px + q$ über $\mathbb{R}$, der Einfachheit halber mit komplexen Nullstellen. Wenn $\alpha = u + vi$ eine Nullstelle ist, dann ist auch $\bar{\alpha} = u - vi$ eine Nullstelle. Das ist manchmal praktisch. Wir suchen also alle Analoga zur komplexen Konjugation in endlichen Körpern.
Was kann die komplexe Konjugation?

- Sie ist ein Automorphismus von $\mathbb{C}$.
- Reelle Zahlen bleiben fix.

Das heißt, wir suchen analog einen Automorphismus von $\mathbb{F}_{q^m}$ der $\mathbb{F}_q$ fix lässt.

Lemma 1.4. *Sei f ein irreduzibles Polynom in $\mathbb{F}_q[X]$ vom Grad m und $n \in N$. Dann gilt*

$$f \mid X^{q^n} - X \Leftrightarrow m \mid n.$$

Beweis.

- $\Leftarrow$ Nachdem $m \mid n$ folgt mit Satz 1.3, dass $\mathbb{F}_{q^m}$ ein Teilkörper von $\mathbb{F}_{q^n}$ ist. Sei nun α eine Nullstelle von f im Zerfällungskörper von f über $\mathbb{F}_q$. Dann ist $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. Auf Grund der Eindeutigkeit des Teilkörpers (Satz 1.3) ist $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ und somit $\alpha \in \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$. Nachdem $X^{q^n} - X$ über $\mathbb{F}_{q^n}$ in Linearfaktoren zerfällt, ist $\alpha^{q^n} = \alpha$ eine Nullstelle von $X^{q^n} - X$. Wir haben α beliebig gewählt und daher muss f das Polynom $X^{q^n} - X$ teilen.
- $\Rightarrow$ Sei α eine Nullstelle von f im Zerfällungskörper über $\mathbb{F}_q$. Nachdem f das Polynom $X^{q^n} - X$ teilt, ist α auch eine Nullstelle von $X^{q^n} - X$. Daher ist $\alpha \in \mathbb{F}_{q^m}$ und es folgt, dass $\mathbb{F}_q(\alpha)$ ein Teilkörper von $\mathbb{F}_{q^n}$ ist. Schließlich ist $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ und $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ und mit Lemma 1.2 folgt, dass $m \mid n$. □

Lemma 1.5. *Sei $f \in \mathbb{F}_q[X]$ irreduzibel,* $\deg f = m$. *α sei Nullstelle von f in Erweiterung von $\mathbb{F}_q$. Dann gilt:*

$$f = (X - \alpha)(X - \alpha^q)(X - \alpha^{q^2}) \cdots (X - \alpha^{q^{m-1}}).$$

Beweis. $\Phi_q : x \mapsto x^q$ ist ein Homomorphismus. Die Einschränkung von Φ_q auf $\mathbb{F}_q$ ist die identische Abbildung weil $\beta^q = \beta$ für alle $\beta \in \mathbb{F}_q$ gilt.
Sei nun β eine Nullstelle von f. Es gilt:

$$0 = \Phi_q\left(f(\beta)\right) = f\left(\Phi_q(\beta)\right) = f\left(\beta^q\right),$$

also ist β^q eine Nullstelle von f. Wenden wir diese Beziehung wiederholt auf α an, so erhalten wir

$$f(\alpha) = 0 \Rightarrow f(\alpha^q) = 0 \Rightarrow f(\alpha^{q^2}) = 0 \Rightarrow \cdots \Rightarrow f(\alpha^{q^{m-1}}) = 0.$$

Wir nehmen indirekt an, diese Nullstellen wären nicht paarweise verschieden. Das heißt, es gibt $0 \leq j < k < m$ mit $\alpha^{q^j} = \alpha^{q^k}$. Nun setzen wir $\beta := \alpha^{q^j}$ und $l := k - j$. Offensichtlich gilt $\beta = \beta^{q^l}$ und $0 < l < m$.
Das Minimalpolynom von β ist f; β ist aber auch Nullstelle von $X^{q^l} - X$. Daher teilt f das Polynom $X^{q^l} - X$ und laut Lemma 1.4 gilt $m \mid l$. Das ist ein Widerspruch zu $0 < l < m$, also müssen die Nullstellen paarweise verschieden sein und wir haben eine Faktorisierung in Linearfaktoren gefunden. □

Bemerkung. Φ_q erfüllt analoge Eigenschaften zur komplexen Konjugation, denn Φ_q ist ein Automorphismus für $\mathbb{F}_{q^m}$ und er lässt $\mathbb{F}_q$ fix.

Definition (Automorphismengruppe)**.**

$$\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}) := \left\{\varphi \in \mathrm{Aut}(\mathbb{F}_{q^m}) \mid \varphi\,|_{\mathbb{F}_q} = \mathrm{id}_{\mathbb{F}_q}\right\}$$

heißt *Automorphismengruppe* von $\mathbb{F}_{q^m}$ über $\mathbb{F}_q$. Ihre Elemente heißen $\mathbb{F}_q$*-Automorphismen* von $\mathbb{F}_{q^m}$.

Bemerkung. Die Automorphismengruppe ist tatsächlich eine Gruppe bezüglich hintereinanderausführung (Beweis durch Nachrechnen).

Bemerkung. $\Phi_q \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m})$, also auch $(\Phi_q)^j \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m})$ (Beweis durch Induktion).

Satz 1.6 (Automorphismenstruktur)**.** *Sei q eine Primzahlpotenz, $m \in \mathbb{N}$. Dann ist* $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m})$ *eine zyklische Gruppe der Ordnung m, die von $\Phi_q : \mathbb{F}_{q^m} \to F_{q^m}$, $x \mapsto x^q$ erzeugt wird, also:*

$$\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = \left\{\mathrm{id}, \Phi_q, \Phi_q^2, \ldots, \Phi_q^{m-1}\right\}.$$

Beweis. Sei $f \in \mathbb{F}_q[X]$ irreduzibel vom Grad m und $\alpha \in \mathbb{F}_{q^m}$ eine Nullstelle von f. Sei weiters $\varphi \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m})$. Dann gilt

$$0 = \varphi(0) = \varphi\left(f(\alpha)\right) = f\left(\varphi(\alpha)\right),$$

$\varphi(\alpha)$ ist also eine Nullstelle von f. Laut Lemma 1.5 gibt es somit ein $j \in \{0, \ldots, m-1\}$ mit $\varphi(\alpha) = \alpha^{q^j} = \Phi_q^j(\alpha)$.
Sei nun $\beta \in \mathbb{F}_{q^m}$ beliebig mit $\beta = \sum_{k=0}^{m-1} c_k \alpha^k$ für passende $c_k \in \mathbb{F}_q$. Es gilt:

$$\begin{aligned}\varphi(\beta) &= \varphi\left(\sum_{k=0}^{m-1} c_k \alpha^k\right) = \sum_{k=0}^{m-1} c_k \left(\varphi(\alpha)\right)^k \\ &= \sum_{k=0}^{m-1} c_k \left(\Phi_q^j(\alpha)\right)^k = \Phi_q^j\left(\sum_{k=0}^{m-1} c_k \alpha^k\right) = \Phi_q^j(\beta),\end{aligned}$$

das bedeutet, $\varphi = \Phi_q^j$.
Da die $\Phi_q^j(\alpha) = \alpha^{q^j}$ laut Lemma 1.5 paarweise verschieden sind, müssen die Φ_q^j paarweise verschieden sein. Also ist die Ordnung der Automorphismengruppe m. □

Bemerkung. $\Phi_q^m(\beta) = \beta^{q^m} = \beta$ für alle $\beta \in \mathbb{F}_{q^m}$, also ist $\Phi_q^m = \mathrm{id}_{\mathbb{F}_{q^m}}$.

1.4 Basen und andere Darstellungen von Körperelementen

Wir wollen uns nun den verschiedenen Darstellungen widmen und ihre Vorzüge und Nachteile beleuten.

Polynombasen

Für ein irreduzibles Polynom vom Grad m mit einer Nullstelle α ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^m}$. Wir sprechen von der *Polynombasis*.

- Addition ist durch m Additionen im Grundkörper leicht zu realisieren.
- Multiplikation erfordert im Allgemeinen Reduktionen von α^j durch das Minimalpolynom, wobei $j \in \{m, \ldots 2m-2\}$, sowie viele Multiplikationen und Additionen im Grundkörper.
- Berechnung von Φ_q erfordert ebenfalls Reduktionen, denn

$$\Phi_q\left(\sum_{k=0}^{m-1} c_k \alpha^k\right) = \sum_{k=0}^{m-1} c_k \Phi_q\left(\alpha^k\right) = \sum_{k=0}^{m-1} c_k \alpha^{q^k}.$$

Logarithmische Darstellung

Die Einheitengruppe von $\mathbb{F}_{q^m}$ ist zyklisch, das heißt es gibt ein $\beta \in \mathbb{F}_{q^m}$ (ein primitives Element), sodass

$$\mathbb{F}_{q^m}^\times = \{\beta^j \mid 0 \le j \le q^m - 1\}.$$

Für $\gamma = \beta^j$ nenne j den *diskreten Logarithmus* von γ zur Basis β. Wir speichern nur diesen Logarithmus.

- Multiplikation durch Addition der Exponenten und Reduktion modulo q^m ist billig.
- Berechnung von Φ_q erfolgt durch Multiplikation des Exponenten mit q und Reduktion modulo q^m.
- Für die Addition braucht man eine Tabelle $(1 + \beta^j)$ oder man muss mühsam rechnen.

Beispiel. Wir wollen nun den Körper $\mathbb{F}_9$ von oben so darstellen. Dazu suchen wir ein primitives Element. Sei α wie oben eine Nullstelle von X^2+1. Dann erhalten wir, dass $2\alpha+2, \alpha+2, \alpha+1, 2\alpha+1$ die Erzeuger von F_9 sind. Wir setzen nun $\beta = \alpha + 1$ und erhalten

β^0	β^1	β^2	β^3	β^4	β^5	β^6	β^7
1	$\alpha+1$	2α	$2\alpha+1$	2	$2\alpha+2$	α	$\alpha+2$

Normale Basen

Sei $\beta \in \mathbb{F}_{q^m}$. Wir betrachten $\{\alpha, \Phi_q(\alpha), \Phi_q^2(\alpha), \ldots, \Phi_q^{m-1}(\alpha)\}$. Falls diese linear unabhängig über $\mathbb{F}_q$ sind, dann bilden sie eine Basis, die sogenannte *normale Basis*.

- Berechnung von Φ_q geht schnell, da man nur den Koordinatenvektor rotieren muss.
- Addition erfolgt komponentenweise.
- Multiplikation erfordert noch mehr Mühe als bei Polynombasen.

Gibt es normale Basen in jedem $\mathbb{F}_{q^m}$?

Satz 1.7 (Existenz normaler Basen)**.** *Sei q eine Primzahlpotenz, $m \in \mathbb{N}$. Dann gibt es ein $\beta \in \mathbb{F}_{q^m}$, sodass $\{\beta, \Phi_q(\beta), \Phi_q^2(\beta), \ldots, \Phi_q^{m-1}(\beta)\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^m}$ ist.*

Für den Beweis werden Hilfsmittel aus der linearen Algebra benötigt (siehe Anhang A1).

Lemma 1.8 (Artin)**.** *Sei $(G, \cdot)$ eine abelsche Gruppe, K ein Körper und $\varphi_1, \ldots, \varphi_m$ paarweise verschiedene Homomorphismen von $G \to K^\times$. Dann gibt es für jedes Tupel $(a_1, \ldots, a_m) \in K^m \setminus (0, \ldots, 0)$ ein $g \in G$ mit*

$$a_1\varphi_1(g) + \cdots + a_m\varphi_m(g) \neq 0.$$

Beweis. Induktion nach m:

- Für $m = 1$ ist nichts zu zeigen.
- Induktionsschritt $m - 1 \to m$: Annahme: oBdA: $a_1 \neq 0$

  $$a_1\varphi_1(g) + \cdots + a_m\varphi_m(g) = 0.$$

  Da $\varphi_1 \neq \varphi_m$ gibt es ein $h \in G$ mit $\varphi_1(h) \neq \varphi_m(h)$. Betrachte

  $$a_1\varphi_1(hg) + \cdots + a_m\varphi_m(hg).$$

  Falls das ungleich 0 ist sind wir fertig, also nehmen wir an:

  $$a_1\varphi_1(h)\varphi_1(g) + \cdots + a_m\varphi_m(h)\varphi_m(g) = 0.$$

  Wir multiplizieren die erste Gleichung mit $\varphi_m(h)$ und subtrahieren die eben aufgestellte Gleichung:

  $$\begin{aligned} 0 &= a_1 \left(\varphi_m(h) - \varphi_1(h)\right) \varphi_1(g) + \cdots + a_{m-1} \left(\varphi_m(h) - \varphi_{m-1}(h)\right) \varphi_{m-1}(g) \\ &=: b_1\varphi_1(g) + \cdots + b_{m-1}\varphi_{m-1}(g) \end{aligned}$$

  gilt für alle g. Widerspruch zur Induktionsannahme. □

Beweis von Satz 1.7. $\Phi_q : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ ist $\mathbb{F}_q$-Automorphismus, also auch eine $\mathbb{F}_q$-lineare Abbildung. Weiters sind $\{\mathrm{id}, \Phi_q, \ldots \Phi_q^{m-1}\}$ paarweise verschiedene Homomorphismen $\mathbb{F}_{q^m}^\times \to \mathbb{F}_{q^m}^\times$. Also gibt es laut Lemma von Artin kein Tupel $(a_0, \ldots a_{m-1}) \in K^m \setminus \{0, \ldots 0\}$, sodass

$$\sum_{j=0}^{m-1} a_j \Phi_q^j \equiv 0.$$

Das Minimalpolynom von Φ_q hat also Grad $\geq m$. Das charakteristische Polynom von Φ_q hat Grad $\leq m$. Somit gilt: Minimalpolynom $= \pm 1$ charakteristisches Polynom $= X^m - 1$ weil $\Phi_q^m = \mathrm{id}_{\mathbb{F}_{q^m}}$. Laut SatzA1.4 gibt es also ein $\alpha \in \mathbb{F}_{q^m}$, sodass $\alpha, \Phi_q(\alpha), \ldots \Phi_q^{m-1}(\alpha)$ eine Basis von $\mathbb{F}_{q^m}$ bilden. □

Beispiel. Wir wollen wieder den Körper $\mathbb{F}_9$ darstellen. Sei dazu α eine Nullstelle von X^2+1 und $\beta = \alpha + 1$. Wir erhalten, dass $\{\beta, \beta^3\} = \{\alpha+1, 2\alpha+1\}$ eine normale Basis ist.

Darstellung durch Matrizen

Sei $f = \sum_{j=0}^{m} a_j X^j \in \mathbb{F}_q[X]$ irreduzibel und normiert. Betrachte die Matrix:

$$A = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \vdots \\ & & 1 & -a_{m-1} \end{pmatrix}$$

Bestimme das Minimalpolynom von A: Setze $e_1 = (1, 0, \ldots, 0)^t$. Es gilt $Ae_1 = e_2, A^2e_1 = e_3, \ldots, A^{m-1}e_1 = e_m$. Also ist $\{A^j e_1 \mid 0 \le j \le m-1\}$ eine Basis von $\mathbb{F}_q^m$ und laut Satz A1.4 Minimalpolynom $= (-1)^m$ charakteristisches Polynom $= (-1)^m \det(A - XI)$. Also

$$\begin{aligned}
(-1)^m \det(A - XI) = \det(XI - A) &= \begin{vmatrix} X & & & a_0 \\ -1 & \ddots & & \vdots \\ & \ddots & X & a_{m-2} \\ & & -1 & X + a_{m-1} \end{vmatrix} \\
&= X \cdot \begin{vmatrix} X & & & a_1 \\ -1 & \ddots & & \vdots \\ & \ddots & X & a_{m-2} \\ & & -1 & X + a_{m-1} \end{vmatrix} + (-1)^{m+1} a_0 \cdot \begin{vmatrix} X & & \\ -1 & \ddots & \\ & \ddots & X \\ & & -1 \end{vmatrix} \\
&= a_0 + X \cdot \begin{vmatrix} X & & & a_1 \\ -1 & \ddots & & \vdots \\ & \ddots & X & a_{m-2} \\ & & -1 & X + a_{m-1} \end{vmatrix} \\
&= a_0 + a_1 X + \cdots + a_{m-1} X^{m-1} + X^m = f.
\end{aligned}$$

Damit ist das Minimalpolynom von A gleich f.
Rechne in $\left\{\sum_{j=0}^{m-1} a_j A^j \mid a_j \in \mathbb{F}_q\right\}$ mit den üblichen Rechenregeln für Matrizen. Setze $\mathbb{F}_{q^m} \simeq \operatorname{span}\{I, A, A^2, \ldots, A^{m-1}\}$. A verhält sich gleich wie eine abstrakte Nullstelle α von f.

Beispiel. Wir wählen wieder $f = X^2 + 1$ und α eine Nullstelle von f. Die Begleitmatrix von f ist

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

Sei nun I die 2x2 Einheitsmatrix. Dann gibt es folgende Darstellung für $\mathbb{F}_9$:

0	I	$2I$	A	$A+I$	$A+2I$	$2A$	$2A+I$	$2A+2I$
$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$

Kapitel 2

Polynome über endlichen Körpern

2.1 Kreisteilungspolynome und Einheitswurzeln

Definition. Sei K ein Körper, $n \in \mathbb{N}$. Dann heißt der Zerfällungskörper von $X^n - 1$ über K der *n-te Kreisteilungskörper* $K^{(n)}$ über K.
Die Nullstellen von $X^n - 1$ heißen *n-te Einheitswurzeln* über K, sie werden in der Menge $E^{(n)}$ zusammengefasst.

Bemerkung. Für $K = \mathbb{R}$ ist $K^{(n)} = \mathbb{R}(\exp(\frac{2\pi i}{n}))$ und $E^{(n)} = \{\exp(\frac{2k\pi i}{n}) \mid 0 \leq k \leq n-1\}$.

Bemerkung. Wir wissen viel über $\mathbb{F}_q^{(q^m-1)}$. Laut Definition ist das der Zerfällungskörper von $X^{q^m-1} - 1$, also auch der Zerfällungskörper von $X^{q^m} - X$ und somit genau der $\mathbb{F}_{q^m}$.

Definition (Primitive n-te Einheitswurzel)**.** Sei $\zeta \in E^{(n)}$ mit $n = \min\{k \in \mathbb{N} \mid \zeta^k = 1\}$, dann heißt ζ eine *primitive n-te Einheitswurzel*

Satz 2.1 (Struktur der Einheitswurzelgruppe)**.** *Sei K ein Körper der Charakteristik $p \geq 0$ (p prim oder 0) und $n \in \mathbb{N}$.*

1. *Falls $p \nmid n$ (also insbesondere falls $p = 0$), so ist $E^{(n)}$ eine zyklische Gruppe der Ordnung n. Für $\zeta \in E^{(n)}$ gilt: $E^{(n)} = \langle\zeta\rangle \Leftrightarrow n = \min\{k \in \mathbb{N} \mid \zeta^k = 1\}$.*
2. *Falls $n = p^l m$ mit $p \nmid m$, so ist $K^{(n)} = K^{(m)}$ und $E^{(n)} = E^{(m)}$.*

Bemerkung. Der zweite Teil des Satzes sagt aus, dass der Fall $p \mid n$ vollkommen uninteressant ist.

Beweis. 1. Zunächst $p \nmid n$.

- $\left(E^{(n)}, \cdot\right)$ ist eine Gruppe:
  - $1^n = 1 \Rightarrow 1 \in E^{(n)}$, also $E^{(n)} \neq \emptyset$.
  - Seien $x, y \in E^{(n)}$, dann gilt $(xy^{-1})^n = x^n y^{-n} = 1 \cdot 1^{-1} = 1$, das heißt $xy^{-1} \in E^{(n)}$.

  Somit ist $(E^{(n)}, \cdot)$ eine Untergruppe von $(K^{(n)}, \cdot)$.
- $|E^{(n)}| = n$: In $K^{(n)}$ zerfällt $X^n - 1$ in Linearfaktoren:

$$X^n - 1 = (X - \alpha_1) \cdots (X - \alpha_n).$$

Somit ist $E^{(n)} = \{\alpha_1, \ldots, \alpha_n\}$. Die Einheitswurzeln sind paarweise verschieden, weil

$$\mathrm{ggT}\left(X^n - 1, (X^n - 1)'\right) = \mathrm{ggT}\left(X^n - 1, nX^{n-1}\right).$$

Wegen $p \nmid n$ gilt, dass $nX^{n-1} \neq 0$. Ein gemeinsamer Primfaktor u der beiden Polynome würde sowohl X^n als auch $X^n - 1$ teilen, das heißt u wäre eine Einheit. Somit ist der ggT gleich 1.

- $(E^{(n)}, \cdot)$ ist als Untergruppe einer zyklischen Gruppe zyklisch ($(K^{(n)}, \cdot)$ ist zyklisch, vergleiche Algebra).
- $\langle\zeta\rangle = E^{(n)} \Leftrightarrow |\zeta| = n \Leftrightarrow n = \min\{k \in \mathbb{N} \mid \zeta^k = 1\}$.

2. Sei nun $n = p^l m$. Dann gilt $X^n - 1 = (X^m)^{p^l} - 1^{p^l} = (X^m - 1)^{p^l}$ (Frobenius), also $K^{(n)} = K^{(m)}$ und $E^{(n)} = E^{(m)}$. □

Definition. Sei $n \in \mathbb{N}$, K ein Körper der Charakteristik $p \geq 0$, $k \in \mathbb{N}$, dann setze

$$P^{(k)} := \{\beta \in K^{(n)} \mid \beta \text{ ist primitive } k\text{-te Einheitswurzel}\}.$$

Bemerkung. $P^{(k)}$ hängt auch von n ab.

Proposition 2.2. *Sei $n \in \mathbb{N}$, K ein Körper der Charakteristik $p \geq 0$, $p \nmid n$, dann gilt*

$$E^{(n)} = \bigcup_{k|n} P^{(k)}.$$

Beweis.

„$\supseteq$“ Falls $\beta \in P^{(k)}$, dann ist $\beta^k = 1$, also $\beta^n = (\beta^k)^{\frac{n}{k}} = 1$, also $\beta \in E^{(n)}$

„$\subseteq$“ Sei $\beta \in E^{(n)}$, dann teilt die Ordnung von β die Gruppenordnung $|E^{(n)}| = n$. Setze $k = |\beta|$ und es folgt $\beta^k = 1$ und somit $\beta \in P^{(k)}$. □

Proposition 2.3. *Sei $n \in \mathbb{N}$, $k \mid n$, K ein Körper der Charakteristik $p \geq 0$, $p \nmid n$. Dann gilt:*

$$|P^{(k)}| = \varphi(k) \text{ (Eulersche } \varphi\text{-Funktion).}$$

Beweis. Zunächst für $k = n$. $E^{(n)} = \langle\zeta\rangle$, also

$$P^{(n)} = \{\zeta^a \mid 0 \leq a \leq n-1 \text{ mit } |\zeta^a| = n\}.$$

Es gilt $|\zeta^a| = n \Leftrightarrow \mathrm{ggT}(a, n) = 1$ (Denn: Es gilt $\zeta^{al} = 1 \Leftrightarrow n \mid al$ und falls $\mathrm{ggT}(a, n) = 1$ folgt $n \mid l$ Andererseits impliziert $\mathrm{ggT}(a, n) > 1$ und $l \leq n$, dass $n \nmid l$). Somit ist

$$P^{(n)} = \{\zeta^a \mid 0 \leq a \leq n-1 \wedge \mathrm{ggT}(a, n) = 1\}$$

und die Ordnung $|P^{(n)}| = \varphi(n)$.
Sei k nun ein Teiler von n, $n = mk$:

$$X^n - 1 = X^{mk} - 1^m = (X^k - 1)R(X),$$

also zerfällt $X^k - 1$ über $K^{(n)}$ in Linearfaktoren. Somit gilt, dass $K^{(k)} \subseteq K^{(n)}$ und wir verweisen auf obigen Fall. □

Korollar 2.4. $n = \sum_{k|n} \varphi(k)$.

Beweis. Kombiniere die letzten beiden Propositionen. □

Bemerkung. Das Korollar ist viel billiger erhältlich und steht hier nur zur Abrundung.

Definition. Sei $n \in \mathbb{N}$, K ein Körper der Charakteristik $p \geq 0$, $p \nmid n$. Definiere das n-te Kreisteilungspolynom G_n rekursiv durch:

$$G_n(X) := \frac{X^n - 1}{\prod_{\substack{k|n \\ k \neq n}} G_k(X)}.$$

Bemerkung. Das leere Produkt ist per Definition 1.

Proposition 2.5. *Bezeichnungen wie in der Definition, dann gilt für $k \mid n$ in $K^{(n)}$:*

$$G_k(X) = \prod_{\beta \in P^{(k)}} (X - \beta) \quad \textit{und} \quad G_k \in K[X].$$

Beweis. Induktion nach k:

$k = 1$ Trivial.

Induktionsschritt: Die Aussage gelte für alle Teiler von n, die kleiner als k sind.

$$\begin{aligned} X^k - 1 &= \prod_{\substack{\beta \in E^{(n)} \\ \beta^k = 1}} (X - \beta) \\ &= G_k(X) \prod_{\substack{d \mid k \\ d \neq k}} G_d(X) = G_k(X) \prod_{\substack{d \mid k \\ d \neq k}} \prod_{\beta \in P^{(d)}} (X - \beta) \end{aligned}$$

Wir kürzen und erhalten:

$$G_k(X) = \prod_{\substack{\beta \in E^{(n)}, \beta^k = 1 \\ \forall d \mid k, d \neq k : \beta^d \neq 1}} (X - \beta) = \prod_{\beta \in P^{(k)}} (X - \beta).$$

Damit ist klar, dass $G_k \in K^{(n)}[X]$, wir wollen aber $G_k \in K[X]$. Division mit Rest in $K[X]$:

$$X^k - 1 = Q(X) \prod_{\substack{d \mid k \\ d \neq k}} G_d(X) + R(X)$$

Lese diese Gleichung in $K^{(n)}[X]$, wo

$$X^k - 1 = G_k(X) \prod_{\substack{d \mid k \\ d \neq k}} G_d(X) + 0$$

gilt. Wegen der Eindeutigkeit der Division mit Rest folgt $R = 0$ und $Q = G_k(X)$. □

Wie sieht die Primfaktordarstellung von Kreisteilungspolynomen aus?

Bemerkung. G_n ist irreduzibel über $\mathbb{Q}[X]$ (hier ohne Beweis).

Satz 2.6 (Primfaktorzerlegung von Kreisteilungspolynomen über endlichen Körpern)**.** *Sei q eine Primzahlpotenz, $n \in \mathbb{N}$ mit $\mathrm{ggT}(q, n) = 1$. Weiters sei d die Ordnung von $(q + n\mathbb{Z})$ in $(\mathbb{Z}/n\mathbb{Z})^\times$, also $d = \min\{k \in \mathbb{N} \mid q^k \equiv 1 \mod n\}$. Dann ist $G_n(X)$ das Produkt von $\frac{\varphi(n)}{d}$ in $\mathbb{F}_q[X]$ irreduziblen Polynomen vom Grad d, die paarweise teilerfremd sind.*

Bemerkung. $\frac{\varphi(n)}{d}$ ist eine positive ganze Zahl, weil $d = |q + n\mathbb{Z}|$ die Ordnung der Einheitengruppe teilt.

Beweis des Satzes. Sei $k \in \mathbb{N}$ und f ein irreduzibler Teiler von G_n in $\mathbb{F}_q[X]$ vom Grad m. Wir behaupten, dass f in $\mathbb{F}_{q^k}$ genau dann in Linearfaktoren zerfällt, wenn $q^k \equiv 1 \mod n$ ist.
f zerfällt über $\mathbb{F}_{q^k}$ in Linearfaktoren
$\Leftrightarrow$ f hat Nullstelle $\beta \in \mathbb{F}_{q^k}$ (Satz 1.6)
$\Leftrightarrow$ f hat Nullstelle β, mit β ist primitive n-te Einheitswurzel und $\beta^{q^k} = \beta$
$\Leftrightarrow$ f hat Nullstelle β mit β ist primitive n-te Einheitswurzel und $\beta^{q^k - 1} = 1$
$\Leftrightarrow$ f hat Nullstelle β mit $n \mid q^k - 1$
$\Leftrightarrow q^k \equiv 1 \mod n$.
$d = \min\{k \in \mathbb{N} \mid q^k \equiv 1 \mod n\} = \min\{k \in \mathbb{N} \mid f$ zerfällt über $\mathbb{F}_{q^k}$ in Linearfaktoren. $\} = m$.
Also hat jeder irreduzible Faktor von G_n Grad d. Da G_n ein Teiler von $X^n - 1$ ist, sind alle irreduziblen Faktoren paarweise teilerfremd Es gibt also $\frac{\deg G_n}{d} = \frac{\varphi(n)}{d}$ Faktoren. □

Korollar 2.7. *Sei q eine Primzahlpotenz, $n \in \mathbb{N}$ mit $\mathrm{ggT}(n,q) = 1$. $\mathbb{F}_q$ enthält genau dann n-te Einheitswurzeln, wenn $n \mid (q-1)$. (Das hat man vorher auch schon gewusst...)*

2.2 Die Ordnung von Polynomen

Lemma 2.8. *Sei $f \in \mathbb{F}_q[X]$ mit $f(0) \neq 0$ und $\deg f = m$, dann gibt es ein $1 \leq k \leq q^m - 1$ sodass $f \mid X^k - 1$.*

Beweis. $\mathbb{F}_q[X]/(f)$ hat $q^m - 1$ Elemente $\neq 0$. Betrachte die Folge $X^l + (f) \in \mathbb{F}_q[X]/(f)$, $0 \leq l \leq q^m - 1$. Diese Folge hat q^m Elemente.
Es gilt, $X^l + (f) \neq 0$ für alle l, weil sonst $X^l = g(X)f(X)$ in $\mathbb{F}_q[X]/(f)$. Einsetzen von 0 ergibt $0 = g(0)f(0)$. Nachdem $f(0) \neq 0$ muss $g(0) = 0$ und somit gilt $X \mid g(X)$, also $X^{l-1} + (f) = 0$. Aber $X^0 + (f) = 1 + (f) \neq 0$.
Somit hat die Folge q^m Elemente ungleich Null in $\mathbb{F}_q[X]/(f)$. Nachdem $|\mathbb{F}_q[x]/(f)| = q^m$ muss laut Schubfachschluss $X^r \equiv X^s \mod (f)$ für passendes $0 \leq r < s \leq q^m - 1$. Also $f \mid X^s - X^r = X^r(X^{s-r} - 1)$. Da $X \nmid f$ gilt $\mathrm{ggT}(X, f) = 1$ und folglich $f \mid X^{s-r} - 1$. □

Definition. Sei $f \in \mathbb{F}_q[X]$ nicht konstant.

- $\mathrm{ord}(f) := \min\{k \in \mathbb{N} \mid f \text{ teilt } X^k - 1\}$ die *Ordnung von f* über $\mathbb{F}_q$.
- Falls $f = X^l g$ mit $g(0) \neq 0$, so setze $\mathrm{ord}(f) := \mathrm{ord}(g)$.

Proposition 2.9. *Sei $f \in \mathbb{F}_q[X]$ irreduzibel mit $\deg f = m$ und $f(0) \neq 0$ (also $f \neq X$). Sei weiters α eine Nullstelle von f in $\mathbb{F}_{q^m}$. Dann ist die Ordnung von f gleich der Ordnung von α in $\mathbb{F}_{q^m}^\times$.*

Beweis. Es gilt: $f \mid X^l - 1 \Leftrightarrow \alpha^l - 1 = 0 \Leftrightarrow \alpha^l = 1$. Die Ordnung von f ist das minimale l mit $f \mid X^l - 1$; die Ordnung von α in $\mathbb{F}_{q^m}^\times$ das minimale l mit $\alpha^l = 1$. □

Korollar 2.10. *Sei $f \in \mathbb{F}_q[X]$ irreduzibel mit $\deg f = m$ und α eine Nullstelle von f in $\mathbb{F}_{q^m}$ dann ist α genau dann ein primitives Element, wenn die Ordnung $\mathrm{ord}(f) = q^m - 1$ ist.*

Beweis. α ist primitives Element $\Leftrightarrow |\alpha| = |\mathbb{F}_{q^m}^\times| = q^m - 1$. □

Bemerkung. Manchmal werden Polynome vom Grad m der Ordnung $q^m - 1$ als „primitive Polynome“ bezeichnet. (Achtung: Verwechslungsgefahr mit primitiven Polynomen, das heißt Polynomen mit Content 1, über ZPE-Ringen!)

Korollar 2.11. *Sei $f \in \mathbb{F}_q[X]$ ein irreduzibles Polynom vom Grad m, dann gilt $\mathrm{ord}(f) \mid q^m - 1$.*

Beweis. Ordnung von α in der Proposition ist Teiler der Gruppenordnung $q^m - 1$. □

Lemma 2.12. *Sei K ein Körper, $m, n \in \mathbb{N}$, dann gilt:*

$$(X^m - 1) \mid (X^n - 1) \Leftrightarrow m \mid n.$$

Beweis. $\Rightarrow$ Division mit Rest in $\mathbb{N}$ ergibt $n = mq + r$ (q ist hier keine Primzahlpotenz!). Es gilt:

$$\begin{aligned} X^n - 1 &= X^{mq+r} - 1 \\ &= X^r(X^{mq} - 1) + (X^r - 1) \\ &= X^r(X^m - 1)(X^{m(q-1(} + X^{m(q-2)} + \ldots + 1) + (X^r - 1). \end{aligned}$$

Falls $X^m - 1$ ein Teiler von $X^n - 1$ ist, dann muss es auch ein Teiler von $X^r - 1$ sein. Das bedeutet entweder $m = \deg(X^m - 1) \leq \deg(X^r - 1) = r$, was im Widerspruch zur Wahl von r steht, oder $r = 0$. Also muss $r = 0$ sein und es gilt $m \mid n$.

$\Leftarrow$ Schon oft verwendet: $X^n - 1 = X^{mt} - 1 = (X^m - 1)(X^{m(t-1)} + X^{m(t-2)} + \ldots + 1)$. □

Korollar 2.13. $\mathrm{ggT}(X^m-1, X^n-1) = X^{\mathrm{ggT}(m,n)}-1$.

Beweis. Wir wissen: $(X^k-1) \mid \mathrm{ggT}(X^m-1, X^n-1) \Leftrightarrow k \mid \mathrm{ggT}(m,n)$. Es bleibt also nur noch zu zeigen, dass der ggT die Form X^k-1 hat.
Ohne Beschränkung der Allgemeinheit sei $n > m$. Induktion über m:

$m = 1$: $\mathrm{ggT}(X-1, X^n-1) = X-1$.

$m-1 \to m$: Für $n = mt + r$ gilt

$$\mathrm{ggT}(X^m-1, X^n-1) = \mathrm{ggT}(X^m-1, X^{n-tm}-1) \qquad \text{(Euklidscher Algorithmus)}$$

und wir können die Induktionsvorraussetzung anwenden. □

Proposition 2.14. *Seien $f, g \in \mathbb{F}_q[X]$ mit $\mathrm{ggT}(f,g) = 1$, $f(0) \neq 0$ und $g(0) \neq 0$, dann gilt:*

$$\mathrm{ord}(fg) = \mathrm{kgV}(\mathrm{ord}(f), \mathrm{ord}(g)).$$

Beweis. Sei $h = fg$. Wenn h das Polynom $X^e - 1$ teilt, dann auch f und g, also $f \mid \mathrm{ggT}(X^e - 1, X^{\mathrm{ord}\, f} - 1)$ beziehungsweise $g \mid \mathrm{ggT}(X^e-1, X^{\mathrm{ord}\, g}-1)$. Der ggT ist aber bekannt, also gilt $f \mid X^{\mathrm{ggT}(e, \mathrm{ord}\, f)} - 1$. Es muss also $\mathrm{ggT}(e, \mathrm{ord}\, f) = \mathrm{ord}\, f$ sein. Analog dazu ist $\mathrm{ggT}(e, \mathrm{ord}\, g) = \mathrm{ord}\, g$. Somit sind sowohl $\mathrm{ord}\, f$ als auch $\mathrm{ord}\, g$ Teiler von e, also ist e ein Vielfaches von $\mathrm{ord}\, f$ und $\mathrm{ord}\, g$. Nachdem $\mathrm{ord}\, h$ das kleinste solche e ist, folgt, dass $\mathrm{ord}\, h = \mathrm{kgV}(\mathrm{ord}\, f, \mathrm{ord}\, g)$. □

Proposition 2.15. *Sei $f \in \mathbb{F}_{p^n}[X]$ irreduzibel, $f(0) \neq 0$ und $b \in \mathbb{N}$. Sei t minimal mit der Eigenschaft $p^t \geq b$. Dann gilt:*

$$\mathrm{ord}(f^b) = \mathrm{ord}(f) p^t.$$

Beweis. Definiere $g := f^b$, $k := \mathrm{ord}\, f$ und $l = \mathrm{ord}\, g$. Wir wissen, dass $f \mid X^k - 1$ und $g \mid X^l - 1$, also teilt auch f das Polynom $X^l - 1$ und somit gilt $k \mid l$.
Außerdem wissen wir, dass $f^b \mid (X^k-1)^b$, also auch $g \mid (X^k-1)^b (X^k-1)^{p^t - b}$, was mittels Frobenius-Homomorphismus zu $X^{kp^t} - 1$ vereinfacht werden kann. Damit wissen wir, dass $l \mid kp^t$, also $l = kp^j$ für ein $0 \leq j \leq t$.
Angenommen $j < t$, also $p^j < b$. Es gilt $f^b \mid X^{kp^j} - 1 = (X^k-1)^{p^j}$. Das geht sich nicht aus, wenn f das Polynom $X^k - 1$ nur einmal teilt, also gilt $f^2 \mid X^k - 1$. Allerdings hat $X^k - 1$ keine mehrfachen Nullstellen, weil $(X^k-1)' = kX^{k-1} \neq 0$ für Nullstellen von $X^k - 1$ ist. Damit haben wir einen Widerspruch hergestellt, also ist $j = t$. □

Satz 2.16 (Ordnung von Polynomen)**.** *Sei $f \in \mathbb{F}_q[X]$, $f = f_1^{b_1} \cdots f_r^{b_r}$ mit paarweise verschiedenen irreduziblen $f_j \in \mathbb{F}_q[X]$. Sei weiters $t \in \mathbb{N}$ minimal mit $p^t \geq \max_{1 \leq j \leq r} b_j$, wobei $p = \chi(\mathbb{F}_q)$. Dann gilt*

$$\mathrm{ord}(f) = p^t \,\mathrm{kgV}(\{\mathrm{ord}(f_j)\}) \mid 1 \leq j \leq r\}).$$

Beweis. Es gilt

$$\begin{aligned}\mathrm{ord}(f) &= \mathrm{kgV}(\{\mathrm{ord}(f_j^{b_j}) \mid j \in \{1, \ldots, r\}\}) \\ &= \mathrm{kgV}(\{\mathrm{ord}(f_j) p^{t_j} \mid j \in \{1, \ldots, r\}\}),\end{aligned}$$

wobei $t_j \in \mathbb{N}$ minimal mit $p^{t_j} > b_j$. Wir wissen $\mathrm{ord}(f_j) \mid q^{\deg f_j} - 1$, daher $\mathrm{ggT}(p, \mathrm{ord}(f_j)) = 1$. Also gilt

$$\begin{aligned}\mathrm{ord}(f) &= \mathrm{kgV}(\{\mathrm{ord}(f_j) \mid j \in \{1, \ldots, r\}) \cdot \mathrm{kgV}(\{p^{t_j} \mid j \in \{1, \ldots, r\}\}) \\ &= \mathrm{kgV}(\{\mathrm{ord}(f_j) \mid j \in \{1, \ldots, r\}) \cdot p^{\max\{t_j\}} \\ &= \mathrm{kgV}(\{\mathrm{ord}(f_j)\}\} \cdot p^t. \square\end{aligned}$$

Proposition 2.17. *Sei q eine Primzahlpotenz, $m \in \mathbb{N}$, $e \in \mathbb{N}$ mit $e \mid q^m - 1$. Dann gibt es genau $\frac{\varphi(e)}{d}$ irreduzible Polynome $f \in \mathbb{F}_q[X]$ vom Grad m der Ordnung e, wobei $d = m$ die Ordnung von $q \mod e$ ist.*

Beweis. f ist irreduzibles Polynom mit $\deg(f) = m$ und $\mathrm{ord}(f) = e \Leftrightarrow$ Nullstelle von f ist primitive e-te Einheitswurzel in $\mathbb{F}_{q^m}$. Daher ist f einer der irreduziblen Teiler von G_e. □

2.3 Irreduzible Polynome

Definition. Sei $\mu : \mathbb{N} \to \mathbb{N}$ eine arithmetische Funktion, sodass

$$\mu(p_1 \cdots p_r) = \begin{cases} (-1)^r & \text{falls } r \geq 0 \text{ und } p_1, \ldots p_r \text{ paarweise verschiedene Primzahlen sind} \\ 0 & \text{sonst.} \end{cases}$$

Dann nennt man μ die MÖBIUSsche μ-Funktion.

Satz 2.18. *Sei q eine Primzahlpotenz und $n \in \mathbb{N}$. Dann ist die Anzahl der normierten irreduziblen Polynome in $\mathbb{F}_q[X]$ vom Grad n gleich*

$$\frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Beweis. Sei $N_q(n)$ die Anzahl der normierten irreduziblen Polynome vom Grad n in $\mathbb{F}_q[X]$. Wir betrachten

$$P := \prod_{\substack{f \in \mathbb{F}_q[X] \text{ irreduzibel} \\ \deg(f) | n \\ f \text{ normiert}}} f.$$

Wir wissen: $f \mid X^{q^n} - X \Leftrightarrow \deg f \mid n$ für irreduzibles f. Jeder Faktor im Produkt P teilt also $X^{q^n} - X$. Jeder Faktor von $X^{q^n} - X$ kommt im Produkt P vor. Also haben P und $X^{q^n} - X$ die gleichen Primfaktoren, aber vielleicht nicht mit denselben Vielfachheiten.
In P kommt laut Konstruktion jeder Primfaktor genau einmal vor. $X^{q^n} - X$ hat ebenfalls keine mehrfachen Primfaktoren, weil $\left(X^{q^n} - X\right)' = q^n X^{q^n - 1} - 1 = -1$.
Da P und $X^{q^n} - X$ beide normiert sind, folgt

$$P = X^{q^n} - X.$$

Sortiere P nach Graden:

$$X^{q^n} - X = \prod_{d|n} \prod_{\substack{f \in \mathbb{F}_q[X] \text{ irreduzibel} \\ \deg(f) = d \\ f \text{ normiert}}} f.$$

Berechne den Grad auf zwei Arten (inneres Produkt hat $N_q(d)$ Faktoren):

$$q^n = \sum_{d|n} d N_q(d).$$

Möbiusinversion (Übung):

$$F(n) = \sum_{d|n} f(d) \Rightarrow f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

In unserem Fall ist also

$$n N_q(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Dividiere durch n. □

Beispiel.

$$\begin{aligned} N_q(12) &= \frac{1}{12} \sum_{d \in \{1,2,3,4,6,12\}} \mu\left(\frac{12}{d}\right) q^d \\ &= \frac{1}{12} \left(\mu(1)q^{12} + \mu(2)q^6 + \mu(3)q^4 + \mu(4)q^3 + \mu(6)q^2 + \mu(12)q\right) \\ &= \frac{1}{12} \left(q^{12} - q^6 - q^4 + q^2\right) \end{aligned}$$

Korollar 2.19. *Für jedes $n \in \mathbb{N}$ existiert ein irreduzibles Polynom vom Grad n in $\mathbb{F}_q[X]$.*

Beweis.

$$\begin{aligned} N_q(n) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d &= \frac{1}{n}\left(q^n + \sum_{\substack{d|n\\ d\neq n}}\mu\left(\frac{n}{d}\right)q^d\right) \\ &\geq \frac{1}{n}\left(q^n + \sum_{\substack{d|n\\ d\neq n}}(-1)q^d\right) \\ &\geq \frac{1}{n}\left(q^n - \sum_{d=1}^{n} q^d\right) = \frac{1}{n}\left(q^n - \frac{q^n - q}{q-1}\right) \\ &> \frac{1}{n}\left(q^n - \frac{q^n}{1}\right) = 0 \end{aligned}$$

□

Bemerkung. Eigentlich kannten wir das Resultat bereits, weil $\mathbb{F}_{q^n}$ bekannterweise existiert und einfache algebraische Körpererweiterung von $\mathbb{F}_q$ ist, muss es ein Minimalpolynom vom Grad n geben.

2.4 Faktorisierung von Polynomen (Berlekamp-Algorithmus)

Bevor wir uns der Faktorisierung von Polynomen widmen, wollen wir zuerst überlegen, ob wir das Problem nicht vereinfachen können. Hierzu wollen wir die Bezeichnung quadratfrei einführen.

Definition. $f \in \mathbb{F}_q[X]$ heißt *quadratfrei*, wenn es kein nicht konstantes $g \in \mathbb{F}_q[X]$ mit $g^2 \mid f$ gibt.

Die Idee ist nun, zu zeigen, dass wir jede Faktorisierung eines beliebigen Polynoms auf die eines quadratfreien Polynoms reduzieren können. Dies ermöglicht uns das folgende Lemma.

Lemma 2.20. *Wenn man das Faktorisierungsproblem für quadratfreie f beherrscht, dann beherrscht man es auch für beliebige f.*

Beweis. $f = \sum_{j=0}^{n} a_j X^j$ sei ein beliebiges Polynom. Betrachte f'.

1. $f' = \sum_{j=1}^{n} j a_j X^{j-1} = 0$. Dann muss $j a_j = 0$ für $0 \leq j \leq n$, also $a_j = 0$ oder $j = 0$, das bedeutet $a_j = 0$ oder $p \mid j$. Somit gilt:

   $$f = \sum_{\substack{j=0\\ p|j}}^{n} a_j X^j = \sum_{i=0}^{\lfloor \frac{n}{p} \rfloor} a_{ip} X^{ip} = \sum_{i=0}^{\lfloor \frac{n}{p} \rfloor} b_i^p (X^i)^p$$

   für passende b_i (siehe Übung).

   Somit ist $f = g^p$ für $g = \sum_{i=0}^{\lfloor \frac{n}{p} \rfloor} b_i X^i$. Faktorisiere g und potenziere die erhaltene Faktorisierung mit p.

2. $f' \neq 0$ und $d = \mathrm{ggT}(f, f')$ ist nicht konstant. dann ist d ein Polynom mit Grad $1 < \deg d \leq \deg f' \leq \deg f$ und $d \mid f$. Schreibe $f = d\frac{f}{d}$ und bastle die Faktorisierung von f aus den Faktorisieungen von d und $\frac{f}{d}$, die beide kleineren Grad haben, zusammen.

3. $f' \neq 0$ und $\mathrm{ggT}(f, f') = \mathrm{const}$. Dann ist f quadratfrei und wir müssen wirklich arbeiten. □

Damit ist klar, dass wir uns im folgenden auf quadratfreie Polynome konzentrieren können. Die zentrale Idee des Berlekamp-Algorithmus ist folgender Satz.

Satz 2.21. *Sei $f \in \mathbb{F}_q[X]$ normiert und $Q \in \mathbb{F}_q[X]$, sodass $Q^q \equiv Q \mod f$. Dann*

$$f(x) = \prod_{\alpha \in \mathbb{F}_q} \mathrm{ggT}(f(x), Q(x) - \alpha).$$

Beweis. Wir zeigen, dass die rechte Seite die linke teilen muss und umgekehrt.
Jeder ggT auf der rechten Seite teilt $f(x)$. Nachdem die Polynome $Q(X) - \alpha$ für $\alpha \in \mathbb{F}_q$ paarweise relativ prim sind, folgt, dass auch das Produkt der ggT $f(x)$ teilt.
Nachdem $h^q \equiv h \mod f$ ist, folgt, dass $f(X)$

$$Q(X)^q - Q(X) = \prod_{\alpha \in \mathbb{F}_q} (Q(X) - \alpha)$$

teilt. Somit teilt $f(x)$ die rechte Seite.
Nun ist f normiert und die beiden Seiten teilen einander. Also bleibt ihnen nichts anderes übrig, als gleich zu sein. □

Mit diesem Satz bekommen wir eine erste Faktorisierung. Diese ist aber nicht vollständig, weil einerseits die Faktoren auf der rechten Seite reduzibel in $\mathbb{F}_q[X]$ sein können und andererseits $Q(X) \equiv c \mod f(X)$ sein kann und wir somit eine triviale Faktorisierung erhalten.
Das heißt unser Ziel wird es sein, Polynome $Q(X)$ zu suchen, die keine triviale Faktorisierung liefern. Sei nun

$$f = f_1 \cdots f_r$$

die gesuchte Faktorisierung von f in irreduzible Faktoren f_i. Dann suchen wir $Q \in \mathbb{F}_q[X]$, sodass $Q(X) \equiv \alpha_i \mod f_i(X)$ und $\deg Q < \deg f$. Diese Polynome erfüllen

$$Q(X)^q \equiv \alpha_i^q \equiv \alpha_i \equiv Q(X) \mod f_i(X) \quad \text{für } 1 \le i \le r.$$

Somit gilt

$$Q(X)^q \equiv Q(X) \mod f(X) \quad \text{und} \quad \deg h < \deg f. \tag{1}$$

Wir wollen nun zeigen, dass diese Polynome einen Vektorraum über $\mathbb{F}_q$ bilden.

Proposition 2.22. *Sei $f \in \mathbb{F}_q[X]$ quadratfrei mit $f = f_1 \cdots f_r$ für irreduzible Polynome f_i. Dann ist*

$$V_f := \{Q \in \mathbb{F}_q[X] \mid \deg Q < \deg f \text{ und } Q^q \equiv Q \mod f\}$$

ein r-dimensionaler $\mathbb{F}_q$-Vektorraum.

Beweis. 1. V_f ist ein $\mathbb{F}_q$-Vektorraum: Seien $Q_1, Q_2 \in V_f$, $\alpha, \beta \in \mathbb{F}_q$ und $Q := \alpha Q_1 + \beta Q_2$. Es gilt:

- $\deg Q \le \max(\deg Q_1, \deg Q_2) < \deg f$
- $Q^q = (\alpha Q_1 + \beta Q_2)^q \equiv \alpha^q Q_1^q + \beta^q Q_2^q \equiv \alpha Q_1 + \beta Q_2 = Q \mod f$.

2. V_f hat die Dimension r über $\mathbb{F}_q$: Sei Z eine unbestimmte über $\mathbb{F}_q$. Wir wissen:

$$Z^q - Z = \prod_{\alpha \in \mathbb{F}_q} (Z - \alpha).$$

Sei $Q \in V_f$ und setze $Z := Q(X)$. Es gilt $f \mid Q(X)^q - Q(X) = \prod_{\alpha \in \mathbb{F}_q} (Q(X) - \alpha)$.

Sei $j \in \{1, \ldots, r\}$. Offensichtlich gilt $f_j \mid \prod_{\alpha \in \mathbb{F}_q} (Q(X) - \alpha)$. Also gibt es ein $\alpha_j \in \mathbb{F}_q$ mit $f_j \mid Q(X) - \alpha_j$, und damit $Q(X) \equiv \alpha_j \mod P_j$. Dieses α_j ist aufgrund der Eindeutigkeit der Division mit Rest eindeutig bestimmt.

Wir betrachten nun die Abbildung $\Phi : V_f \to \mathbb{F}_q^r, Q \mapsto (\alpha_1, \ldots, \alpha_r)$ mit $Q(X) \equiv \alpha_j \mod P_j$ für $1 \le j \le r$.

- Φ ist injektiv: Seien $Q_1, Q_2 \in V_f$ mit $\Phi(Q_1) = \Phi(Q_2)$. Dann gilt $Q_1(X) \equiv Q_2(X) \mod f_i$, also $f_i \mid (Q_1 - Q_2)$ für $1 \leq i \leq r$. Also muss auch $f \mid (Q_1 - Q_2)$ gelten. Weil $\deg(Q_1 - Q_2) < \deg f$ ist $Q_1 = Q_2$.
- Φ ist surjektiv: Sei $(\alpha_1, \ldots, \alpha_r) \in \mathbb{F}_q^r$, dann gibt es ein $Q \in \mathbb{F}_q[X]$ mit $Q \equiv \alpha_i \mod P_i$ (chinesischer Restsatz).
  OBdA gilt $\deg Q < \deg f$, sonst Division mit Rest durch f. $Q^q \equiv \alpha_i^q = \alpha_i \equiv Q \mod f_i$, also $Q^q \equiv Q \mod f$ und somit $Q \in V_f$. Daher ist Φ surjektiv.

Also hat V_f die selbe Kardinalität wie $\mathbb{F}_q^r$, nämlich q^r und somit Dimension r. □

Nachdem V_f ein Vektorraum der Dimension r über $\mathbb{F}_q$ ist, gibt es q^r Lösungen für unsere Gleichung in (1). Wir wollen diese Gleichung nun mit folgendem Lemma auf ein System linearer Gleichungen reduzieren.

Lemma 2.23. *Sei $f \in \mathbb{F}_q[X]$, $\deg f = n$ und $X^{lq} \equiv q_{0,l} + q_{1,l}X + \cdots + q_{n-1,l}X^{n-1} \mod f$ für $0 \leq l < n$. Setze $Q_f := (q_{k,l})_{0 \leq k,l \leq n-1} \in \mathbb{F}_q^{n \times n}$. Seien $b^{(1)}, \ldots, b^{(r)}$ ein Basis des Eigenraumes von Q_f zum Eigenwert 1, $b^{(i)} = (b_0^{(i)}, \ldots, b_{n-1}^{(i)})^t$ und V_f wie in der vorhergehenden Proposition definiert.*
Dann ist $\sum_{j=0}^{n-1} b_j^{(i)} X^j, 1 \leq i \leq r$ eine Basis von V_f.

Beweis.

$$V_f = \{Q(x) \mid \deg Q < n, Q^q \equiv Q \mod f\}.$$

Sei $Q(x) = \sum_{j=0}^{n-1} a_j X^j$.

$$\begin{aligned}
Q \in V_f &\Leftrightarrow Q^q \equiv Q \mod f & &\Leftrightarrow \left(\sum_{j=0}^{n-1} a_j X^j\right)^q \equiv \sum a_j X^j \mod f \\
&\Leftrightarrow \sum_{j=0}^{n-1} a_j X^{jq} \equiv \sum a_j X^j \mod f & &\Leftrightarrow \sum_{j=0}^{n-1} a_j \sum_{k=0}^{n-1} q_{k,j} X^k \equiv \sum_{j=0}^{n-1} a_j X^j \mod f \\
&\Leftrightarrow \sum_{k=0}^{n-1} \left(\sum_{j=0}^{n-1} q_{k,j} a_j\right) X^k \equiv \sum_{k=0}^{n-1} a_k X^k \mod f & &\Leftrightarrow \sum_{k=0}^{n-1} \left(\sum_{j=0}^{n-1} q_{k,j} a_j\right) X^k = \sum_{k=0}^{n-1} a_k X^k \\
&\Leftrightarrow \sum_{j=0}^{n-1} q_{k,j} a_j = a_k & &\Leftrightarrow Q_k \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} = 1 \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} \\
&\Leftrightarrow \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} \text{ ist EV zum EW 1 von } Q_f. &&
\end{aligned}$$

Basis von $V_f \leftrightarrow$ Basis des Eigenraums. □

Für den Berlekamp Algorithmus siehe Abbildung 2.1.

Bemerkung.

- $\mathrm{Ker}(Q_f - I_n)$ ist Eigenraum zum Eigenwert 1 von Q_f.
- Nachdem das Polynom $Q(x) = 1$ sicher eine Lösung ist ($1^q \equiv 1 \mod f$), ist $b^{(1)} = (1, 0, \ldots, 0)^t$ sicher im $\mathrm{Ker}(Q_f - I_n)$
- B_i sind lt. Lemma Basis von V_f.
- F: im aktuellen Schritt noch nicht betrachtete Faktoren von f.

- G: im aktuellen Schritt bereits betrachtete Faktoren von f.

Satz 2.24. *Der Berlekamp-Algorithmus terminiert und ist korrekt.*

Beweis. Nach $(r+1)q(r-1)$ Durchläufen der `while`-Schleife ist spätestens Schluss.
Falls das `Return`-Statement nicht genutzt wird, so ist Ergebnis undefiniert. Immer (vor dem `if` $|F \cup G| = r$) gilt

- $$\prod_{g \in F} g \cdot \prod_{g \in G} g = f$$

  (leichteste Induktion).

- $\forall g \in F \cup G : \deg g \geq 1$.

(„Das wird schon stimmen, sonst stürz ich halt mit einem Bluescreen ab.“)
Falls wir über `Return` aussteigen, haben wir Faktorisierung von f in r nicht-konstante Polynome gefunden. Da lt. Vor. f nur r irreduzible Faktoren hat, müssen alle gefundenen Faktoren diese irreduzible Faktoren sein. („Bis jetzt nur Trivialbeobachtungen ohne auf die B_s genauer einzugehen.“)
Zu zeigen bleibt, dass zwei Primfaktoren P_i und P_j, $i \neq j$, in irgendeinem Schritt tatsächlich getrennt werden, d.h.

$$f_i \mid \mathrm{d} \quad \text{und} \quad f_j \mid \frac{g}{d}.$$

Behauptung: Es gibt ein $2 \leq s \leq r$, ein $\alpha_i \neq \alpha_j \in \mathbb{F}_q$ mit

$$B_s \equiv \alpha_i \mod f_i, \qquad B_s \equiv \alpha_j \mod f_j.$$

Wir wissen: Es gibt ein $Q = \sum_{s=1}^{r} \beta_s B_s \in V_f$ mit

$$Q \equiv \alpha_i \mod f_i, \qquad Q \equiv \alpha_j \mod f_j$$

für verschiedene $\alpha_i \neq \alpha_j$. Annahme:

$$B_s \equiv \gamma_s \mod f_i, \qquad B_s \equiv \gamma_s \mod f_j$$

für $1 \leq s \leq r$ und passende $\gamma_s \in \mathbb{F}_q$ ($\gamma_1 = 1$). Also folgt

$$Q \equiv \sum \beta_s \gamma_s \mod f_i, \qquad Q \equiv \sum \beta_s \gamma_s \mod f_j.$$

Widerspruch zu $\alpha_i \neq \alpha_j$.
Falls f_i und f_j beim Schleifendurchlauf für dieses s und dieses α_i noch nicht getrennt sind $\Rightarrow$ $f_i \mid B_s - \alpha_i$, aber $f_i \mid d$. $f_j \nmid B_s - \alpha_i$ (sonst $f_j \mid B_s - \alpha_j$ und $f_j \mid B_s - \alpha_i$ und somit $f_j \mid \alpha_j - \alpha_i$, eine Konstante $\neq 0$, Widerspruch).
Das heißt $f_j \nmid d$, also $f_j \mid \frac{g}{d}$. □

Gegeben: $f \in \mathbb{F}_q[X]$ quadratfrei.

Gesucht: $f = f_1 \cdots f_r$ mit irreduziblen $f_i \in \mathbb{F}_q[X]$.

Algorithmus:

$n = \deg f$
Setze $Q_f = (q_{k,\ell})_{0 \le k,\ell, \le n-1} \in \mathbb{F}_q^{n \times n}$, sodass

$$X^{\ell q} \equiv q_{0,\ell} + \cdots + q_{n-1,\ell} X^{n-1} \pmod{f}.$$

Wähle Basis $b^{(1)}, \ldots, b^{(r)}$ von $\ker(Q_f - I_n)$ (Gauß-Elimination), wobei $b^{(1)} = (1, 0, \ldots, 0)^t$.
$B_i = \sum_{j=0}^{n-1} b_j^{(i)} X^j$.
$G = f$.
for all $0 \le s \le r$ **do**
  for all $\alpha \in \mathbb{F}_q$ **do**
    $F = G$.
    $G = \emptyset$.
    while $F \neq \emptyset$ **do**
      Wähle $g \in F$.
      $F = F \setminus \{g\}$.
      $d = \mathrm{ggT}(B_s - \alpha, g)$.
      if $1 \le \deg d < \deg g$ **then**
        $G = G \cup \{d, g/d\}$.
      else
        $G = G \cup \{g\}$.
      end if
      if $|F \cup G| = r$ **then**
        Return $F \cup G$.
      end if
    end while
  end for
end for

Abbildung 2.1: Berlekamp Algorithmus

Kapitel 3

Grundbegriffe der Codierungstheorie

3.1 Einführung

- ISBN10 (International Standard Book Number):
  - $\underbrace{3}_{\text{deutsch}}$ - $\underbrace{540}_{\text{Springer Verlag}}$ -$\underbrace{64133}_{\text{Buch}}$- $\underbrace{5}_{\text{Prüfziffer}}$
  - bzw. 0-387-64133-5
  - 3-540-97329-X

  funktioniert modulo 11 (X=10).
- ISBN13 (= EAN):
  - $\underbrace{978}_{\text{book land}}$ 3540 64133 9
  - $\underbrace{49}_{\text{Japan}}$ 02778 91395 $\underbrace{3}_{\text{Prüfziffer}}$

  Überprüfung von EAN bzw. ISBN13:

  $$(1,3,1,\ldots,3,1,3,1)\cdot(9,7,8,3,5,4,0,6,4,1,3,3,9)^t \equiv 0 \mod 10.$$

  Bei Überprüfung werden einfache Fehler erkannt:
  - Eine Ziffer falsch:

    $$x \equiv y \mod 10 \text{ oder } 3x \equiv 3y \mod 10 \Rightarrow x = y.$$

  - die meisten Ziffernstürze.

  Nicht erkannt:
  - Vertauschen zweier nenbeneinanderliegender Ziffern, wenn sie kongruent $\mod 5$ sind:

    $$3x + y \equiv x + 3y \mod 10 \Leftrightarrow 2x \equiv 2y \mod 10 \Leftrightarrow x \equiv y \mod 5.$$

  Prüfziffer ist relativ billig: Informationsrate $\frac{12}{13}$.
- IBAN (International Bank Account Number): komische Manipulation, dann $\mod 97$.

- ÖBB-Lokomotiven: $\underbrace{1116}_{\text{Reihe}}\text{-}\ \underbrace{077}_{\text{Ordnungsnr.}}\ \text{-}\ \underbrace{7}_{\text{Prüfziffer}}$.

$$(1,1,1,6,0,7,7)\cdot\begin{pmatrix}0\\1\\2\\1\\2\\1\\2\end{pmatrix}+\mathrm{PZ}\equiv 0 \mod 10.$$

Bis jetzt: Prüfziffer gegen menschliche Irrtümer.
Aber auch:

- Festplatten: Jeder 512 Byte Block braucht ca. 540 Bytes. (CRC = „cyclic redundancy check“)
- ECC-Memory: 1-Bit-Fehler korrigieren, 2-Bit-Fehler erkennen
- Funk

Beispiel. 3 „synthetische“ Codes als Beispiele:

1. Codewörter: $\{0,1\}^8$ (also 8 Bit). Summe der Bits gerade? („Paritätscheck“)
   - 0110101-0
   - 1110000-1

   Erkenne 1-Bit-Fehler.

   7 Bit Nutzdaten, 1 Bit Prüfbit.
2. Codewörter: 3 Bit Länge, alle gleich.
   - 000
   - 111

   1 Bit Nutzdaten, 2 Bit Prüfbits, also kostspielig.

   Erkenne ≤ 2 Bit-Fehler, *oder* (exklusiv) korrigiere 1 Bit-Fehler (Mehrheitsentscheidung; bei Erhalt von z.B. 101 korrigiere auf 111).
3. Codewörter: 6 Bit Länge, *abcxyz*.

$$\begin{aligned} a+b+x &\equiv 0 \mod 2\\ a+c+y &\equiv 0 \mod 2\\ b+c+z &\equiv 0 \mod 2 \end{aligned}$$

   x, y, z sind Prüfbits, a, b, c Nutzdaten.

   Erkenne 2 Bit-Fehler, *oder* korrigiere 1 Bit-Fehler (Nachrechnen oder warten).

3.2 Blockcodes, Distanz, Hamminggewicht

Definition. Sei A eine endliche Menge („Alphabet“) und $m, n \in \mathbb{N}$ mit $m \leq n$. Eine Teilmenge C von A^n der Kardinalität $|C| = |A|^m$ heißt ein (n,m)-*Blockcode*. Eine bijektive Abbildung $E : A^m \to C$ heißt *Codierer für* C (coding scheme), die Umkehrabbildung heißt *Decodierer* (decoding scheme).

Beispiel. alle: $A = \{0,1\}$.

1. $n = 8, m = 7$.

$$\begin{aligned} E :&(x_1, \dots, x_7) \mapsto (x_1, x_2, \dots, x_7, x_1 + x_2 + \cdots + x_7 \mod 2) \\ E^{-1} :&(y_1, \dots, y_7, y_8) \mapsto (y_1, \dots, y_7) \\ C =&\{(y_1, \dots, y_8) \mid y_1 + \cdots + y_8 \equiv 0 \mod 2\}. \end{aligned}$$

2. $n = 3, m = 1$.

$$E : (x) \mapsto (x, x, x).$$

3. $n = 6, m = 3$.

$$E : (a, b, c) \mapsto (a, b, c, a + b \mod 2, a + c \mod 2, b + c \mod 2).$$

Definition. Ein Codierer heißt *systematisch*, falls

$$E(x_1, \dots, x_m) = (x_1, \dots, x_m, z_{m+1}, \dots, z_n)$$

für passende $z_{m+1}, \dots, z_n$ gilt.

Bemerkung. Alle bisher betrachteten Codierer (bis auf IBAN) sind systematisch.

Definition. Sei A eine endliche Menge, $x, y \in A^n$.

1. Die *(Hamming-)Distanz*

$$\mathrm{d}(x, y) := \#\{j \in \{1, \dots, n\} \mid x_j \neq y_j\}$$

ist die Anzahl der Stellen, an denen sich x und y unterscheiden.

2. Das *Hamming-Gewicht* ist definiert als

$$\mathrm{wt}(x) := \mathrm{d}(x, \mathbf{0}),$$

wobei $0 \in A$ und $\mathbf{0} = (0, \dots, 0)$.

Satz 3.1. *Sei A eine endliche Menge und d die Hammingdistanz auf A. Dann ist (A^n, d) ein metrischer Raum.*

Beweis. Offensichtlich gelten

$$\mathrm{d}(x, y) \geq 0, \quad \mathrm{d}(x, y) = 0 \Leftrightarrow x = y \quad \text{und} \quad \mathrm{d}(x, y) = \mathrm{d}(y, x).$$

Es fehlt noch die Dreiecksungleichung. Hierzu seien jetzt $x, y, z \in A^n$. Wir setzen

$$\begin{aligned} M &:= \{j \in \{1, \dots, n\} \mid x_j = y_j \text{ und } x_j \neq z_j\}, \\ N &:= \{j \in \{1, \dots, n\} \mid x_j \neq y_j \text{ und } x_j \neq z_j\}. \end{aligned}$$

Offensichtlich gilt $M \cap N = \emptyset$. Weiters

$$\mathrm{d}(x, z) = \#(M \cup N) = \#M + \#N.$$

Außerdem

$$\#M \leq \mathrm{d}(y, z)$$

(weil $x_j \neq z_j$ und $x_j = y_j \Rightarrow y_j \neq z_j$) und

$$\#N \leq \mathrm{d}(x, y),$$

somit

$$\mathrm{d}(x, z) = \#M + \#N \leq \mathrm{d}(x, y) + \mathrm{d}(y, z). \qquad \square$$

Definition. Die *Minimaldistanz* $\mathrm{d}(C)$ eines Blockcodes C ist als

$$\mathrm{d}(C) := \min\{\mathrm{d}(x,y) \mid x \in C, y \in C, x \neq y\}$$

definiert.

Beispiel. 1. Paritätscheck: $\mathrm{d}(C) = 2$.

$$\mathrm{d}(00000000, 00000011) = 2 \Rightarrow \mathrm{d}(C) \leq 2.$$

Seien $x \neq y \in C$. Wenn $x_j \neq y_j$ für ein $1 \leq j \leq 8$, dann muss es ein $k \neq j$ geben, sodass $x_k \neq y_k$ (Paritätsbedingung), d.h. $\mathrm{d}(x,y) \geq 2$, also $\mathrm{d}(C) \geq 2$.

2. 3-facher Wiederholungscode:

$$\mathrm{d}(111, 000) = 3 \Rightarrow \mathrm{d}(C) = 3.$$

3. $\mathrm{d}(C) = 3$ (ohne Beweis). (Codwörter hinschreiben, alle Paare bilden.)

Definition. Sei C ein (n,m)-Blockcode. ein Fehlerprozessor F ist eine Abbildung

$$F : A^n \to \{\text{wahr}, \text{falsch}\} \times A^n,$$

sodass

$$F(x) = (\text{wahr}, y) \Longrightarrow y \in C.$$

Bemerkung.

$$\underbrace{z \in A^m}_{\text{Nutzdaten}} \xrightarrow{E} x \in C \subseteq A^n \overset{\text{Übertragung, Störung, etc.}}{\longrightarrow} y$$

$$y \xrightarrow{F} \begin{cases} (\text{wahr}, x) \xrightarrow{E^{-1}} E^{-1}(x) = z & \text{Fehler korrigieren} \\ (\text{falsch}, ?) & \text{Fehler erkennen} \\ (\text{wahr}, \tilde{x}) \xrightarrow{E^{-1}} E^{-1}(\tilde{x}) \neq z & \text{unerwünscht} \end{cases}$$

Wir wollen den Fehlerprozessor nun benutzen um Fehler zu erkennen. Dazu müssen wir uns aber zuerst überlegen, was wir unter einem t-Bit-Fehler verstehen.
Wir wollen nun den Begriff der Fehlerkorrektur einführen.

Definition. Sei $t \in \mathbb{N}$ und C ein (n,m)-Blockcode über A. Ein Fehlerprozessor F korrigiert t-Bit-Fehler, wenn es für jedes $y \in A^n$ höchstens ein $c \in C$ gibt, sodass $d(y,c) \leq t$, und

$$F(y) = (\text{wahr}, c).$$

Wenn ein Wort $c \in C$ übertragen wird und dabei t Fehler (t Bits fallen um) auftreten, sodass sich das Wort y ergibt, dann gilt offensichtlich $\mathrm{d}(y,c) \leq t$. Wenn nun C t-Bit-Fehler erkennt, gibt es höchstens ein $c' \in C$ das y am nächsten liegt ($\mathrm{d}(c',y) \leq t$). Dieses c' muss das ursprüngliche c sein.

Proposition 3.2. *Sei C ein (n,m)-Blockcode über A. Dann sind folgende Aussagen äquivalent:*

1. *Es gibt einen Fehlerprozessor, der Fehler bis zum Gewicht s korrigiert.*
2. *$d(C) \geq 2s+1$*

Beweis. Sei $B_s(\mathbf{x})$ eine „Kugel“ in $\mathbb{F}_q^n$ mit Radius s und Mittelpunkt x. Dann gilt offensichtlich $B_s(\mathbf{x}) = \{y \in \mathbb{F}_q^n \mid \mathrm{d}(x,y) \leq s\}$. Um nun t Bit-Fehler zu korrigieren dürfen sich die Kugeln vom Radius s um die Codewörter nicht schneiden. Angenommen es gäbe ein $u \in \mathbb{F}_q^n$ mit $u \in B_s(\mathbf{x}) \cap B_s(\mathbf{y})$, $\mathbf{x} \neq \mathbf{y} \in C$. Dann

$$\mathrm{d}(\mathbf{x}, \mathbf{y}) \leq \mathrm{d}(\mathbf{x}, \mathbf{u}) + \mathrm{d}(\mathbf{y}, \mathbf{u}) \leq 2s,$$

was ein Widerspruch zur Annahme $\mathrm{d}_C \geq 2s+1$ ist. □

Definition. Ein Fehlerprozessor F erkennt t-Bit-Fehler, wenn für alle $x \in C$ und alle $y \in A^n$ mit $\mathrm{d}(x,y) = t$ gilt, dass

$$F(y) = ([x = y], ?).$$

Proposition 3.3. *Sei C ein (n,m)-Blockcode über A und $t \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:*

1. *Es gibt einen Fehlerprozessor F für C, der t-Bit-Fehler erkennt.*
2. $\mathrm{d}(C) \geq t+1$.

Beweis. **1 $\Longrightarrow$ 2:** Sei F so ein Fehlerprozessor. Angenommen, $\mathrm{d}(C) \leq t$. Dann gibt es $c_1, c_2 \in C$ mit $0 < \mathrm{d}(c_1, c_2) \leq t$. c_2 könnte eine fehlerbehaftete Übertragung von c_1 sein, aber

$$F(c_2) = (\text{wahr}, ?).$$

1 $\Longleftarrow$ 2: $\mathrm{d}(c_1, c_2) \geq t+1$.

$$F(y) = ([y \in C], y).$$

□

Satz 3.4. *Sei C ein (n,m)-Blockcode über A, $s,t \in \mathbb{N}_0$. Dann sind folgende Aussagen äquivalent:*

1. *Es gibt einen Fehlerprozessor, der Fehler mit Gewicht $\leq s$ korrigiert und Fehler von Gewicht $\in \{s+1, \ldots, s+t\}$ erkennt.*
2. *$d(C) \geq 2s+t+1$*

Beweisskizze. Für $x, y \in C$:

$$\begin{aligned} & \overline{B(x, s+t)} \cap \overline{B(y,s)} = \emptyset \\ \Leftrightarrow \quad & d(C) > 2s+t \Leftrightarrow d(C) \geq 2s+t+1. \end{aligned}$$

□

Definition (Rate)**.** Sei C ein (n,m)-Blockcode. Dann heißt $\frac{m}{n}$ die *Rate* von C.

Beispiel. 1. Paritätscheck: $\frac{7}{8}$

2. 3-fach-Wiederholung: $\frac{1}{3}$
3. *abcxyz*: $\frac{3}{6} = \frac{1}{2}$

3.3 Lineare Codes

Definition. Sei $\mathbb{F}_q$ ein endlicher Körper, $m, n \in \mathbb{N}$. Ein Unterraum C von $\mathbb{F}_q^n$ der Dimension m („bezieht sich auf C“) heißt *linearer (n,m)-Code über $\mathbb{F}_q$*. Der Codierer $\mathbb{F}_q^m \to \mathbb{F}_q^n$ soll eine lineare Abbildung sein. Falls $q = 2$, spricht man auch von einem *binären linearen Code*. Die Matrixdarstellung des Codierers bzgl. der Standardbasen von $\mathbb{F}_q^m$ bzw. $\mathbb{F}_q^n$ heißt *Generatormatrix* G.

Beispiel. 1. Paritätscheck:

$$\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & & \\ \vdots & 0 & & \vdots \\ & \vdots & & \\ 0 & 0 & & 1 \\ 1 & 1 & & 1 \end{pmatrix} = \begin{pmatrix} I_7 \\ \vec{1}^t \end{pmatrix}$$

2.
$$\begin{pmatrix}1\\1\\1\end{pmatrix}$$

3.
$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\0&1&1\\1&0&1\\1&1&0\end{pmatrix}$$

Bemerkung. C ist systematischer Code $\Longleftrightarrow$ Generatormatrix $= \begin{pmatrix}I_m\\A\end{pmatrix}$ mit $A \in \mathbb{F}_q^{(n-m)\times m}$.

Proposition 3.5. *Sei C ein linearer (n,m)-Code. Dann gibt es eine Matrix M, sodass*

$$x \in C \Leftrightarrow Mx = 0.$$

Jede solche Matrix hat mindestens $n-m$ Zeilen, wobei es auch eine solche Matrix mit $n-m$ Zeilen gibt.

Beweis. Wir benötigen eine lineare Abbildung F von $\mathbb{F}_q^n$ nach $\mathbb{F}_q^n$ mit $C = \operatorname{Ker} F$. Sei $v^1, \ldots, v^m$ eine Basis von C, die durch $v^{m+1}, \ldots, v^n$ zu einer Basis von $\mathbb{F}_q^n$ ergänzt wird. Wähle z.B.

$$F(v^j) = \begin{cases}0 & j \le m\\ e^{j-m} & j > m\end{cases} \text{ mit } e^j = \begin{pmatrix}0\\\vdots\\0\\1\\0\\\vdots\\0\end{pmatrix} \leftarrow j\text{-te Zeile.}$$

Es gilt $\operatorname{Ker} F = C$. ($C \subseteq \operatorname{Ker} F$ lt. Konstruktion. $\operatorname{Im} F = \mathbb{F}_q^{n-m}$. Dimensionsformel: $\dim \operatorname{Ker} F + \underbrace{\dim \operatorname{Im} F}_{=n-m} = n$, somit $\dim \operatorname{Ker} F = m \Rightarrow C = \operatorname{Ker} F$.)
Eine Matrixdarstellung von F bzgl. Standardbasen ergibt die gewünschte Matrix.
Jede solche Matrix hat mindestens $n-m$ Zeilen, weil

$$\operatorname{rank} M = n - \operatorname{Ker} M = n - m. \qquad \square$$

Definition. Eine Matrix mit den Eigenschaften aus der Proposition heißt *Prüfmatrix* (oder *Checkmatrix*, *engl.* parity-check matrix) für C.

Beispiel. 1. Paritätscheck:
$$\begin{pmatrix}1 & \cdots & 1\end{pmatrix}$$

2. 3-fach-Wiederholung:
$$\begin{pmatrix}1&1&0\\1&0&1\end{pmatrix} \text{ oder } \begin{pmatrix}1&0&1\\0&1&1\end{pmatrix}$$

3. *abcxyz*:
$$\begin{pmatrix}1&0&0&0&1&1\\0&1&0&1&0&1\\0&0&1&1&1&0\end{pmatrix}$$

Proposition 3.6. *Sei C ein systematischer linearer (n,m)-Code mit Generatormatrix $\begin{pmatrix} I_m \\ A \end{pmatrix}$, $A \in \mathbb{F}_q^{(n-m)\times m}$. Dann ist $\begin{pmatrix} -A & I_{n-m} \end{pmatrix} \in \mathbb{F}_q^{(n-m)\times m}$ eine Prüfmatrix für C.*

Beweis.

$$\operatorname{rank}\begin{pmatrix} -A & I_{n-m} \end{pmatrix} = n - m \text{ wegen der Einheitsmatrix}$$

$$x \in C \Rightarrow x = \begin{pmatrix} I_m \\ A \end{pmatrix} y \text{ für ein } y \in \mathbb{F}_q^m,$$

somit

$$Mx = \begin{pmatrix} -A & I_{n-m} \end{pmatrix} \begin{pmatrix} I_m \\ A \end{pmatrix} y = (-AI + IA)y = 0,$$

also

$$C \subseteq \operatorname{Ker}\begin{pmatrix} -A & I_{n-m} \end{pmatrix}.$$

Laut Dimensionsformel muss Gleichheit folgen:

$$C = \operatorname{Ker}\begin{pmatrix} -A & I_{n-m} \end{pmatrix}.$$

□

Proposition 3.7. *Sei C ein linearer Code. Dann gilt*

$$\mathrm{d}(C) = \min\{\mathrm{wt}(c) \mid c \in C, c \neq 0\}.$$

(„Statt alle Paare und ihre Differenz zu betrachten, brauche ich nur die c selbst betrachten.“)

Beweis.

$$\mathrm{d}(x,y) = \#\{j \mid x_j \neq y_i\} = \#\{j \mid x_j - y_j \neq 0\} = \mathrm{wt}(x-y).$$

Da C linear ist, ist C ein Unterraum und es gilt für $x, y \in C$ auch $x - y \in C$.

$$\min_{x\neq y, x,y\in C} \mathrm{d}(x,y) = \min_{x\neq y, x,y\in C} \mathrm{wt}(x-y) = \min_{c\neq 0, c\in C} \mathrm{wt}(c)$$

(Jedes $c \in C$ tritt als Differenz auf, z.B. $c - 0$.) □

Bemerkung. Das drückt die Komplexität einer trivialen Suche nach der Hammingdistanz von $|C|^2 - 1$ auf $|C| - 1$.

Fehlererkennung war leicht (Prüfmatrix). Wie soll man Fehler *korrigieren*? Damit meinen wir, zu gegebenem $x \in \mathbb{F}_q^n$ ein $c \in C$ mit $\mathrm{d}(c,x)$ minimal zu finden.

Standard-Tafel

Die Standard-Tafel ist eine Tabelle bestehend aus q^m Spalten und q^{n-m} Zeilen. Jeder Eintrag ist ein Wort aus $\mathbb{F}_q^n$.
Die 1. Zeile besteht aus allen Codewörter

$$x_{11} = 0 \qquad x_{12} \qquad \dots \qquad x_{1q^m}$$

Wähle ein x mit minimalem Gewicht, das noch nicht in der Tafel steht, und notiere

$$x + x_{11} \qquad x + x_{12} \qquad \dots \qquad x + x_{1q^m}.$$

Iteriere (immer 1. Zeile dazuaddieren).
Falls ein Element doppelt vorkommt,

$$x + x_{1k} = x' + x_{1l},$$

so folgt

$$x' = x + (x_{1k} - x_{1l}) = x + x_{1t}$$

für passendes t (Widerspruch).
D.h. in jeder Zeile gilt

$$\mathrm{wt}(x_{k1}) \leq \mathrm{wt}(x_{kj}) \qquad \text{für alle } j.$$

Wir nehmen nun an, dass wir ein x_{kj} empfangen. Dann suchen wir jenes $c \in C$ mit $\mathrm{d}(x_{kj}, c)$ minimal, also $\mathrm{wt}(x_{kj} - c)$ minimal. Die Elemente $x_{kj} - c$, $c \in C$, sind genau die Elemente der k-ten Zeile (aufgrund der Linearität). Suche das Element geringsten Gewichts in der k-ten Zeile. Das erste Element der k-ten Zeile minimiert das.

$$x_{kj} - c = x_{k1},$$

somit

$$c = x_{kj} - x_{k1} = (x_{k1} + x_{1j}) - x_{k1} = x_{1j}.$$

Das gesuchte Codewort ist das erste Element der jeweiligen Spalte.
Die Lösung ist genau dann eindeutig, wenn

$$\mathrm{wt}(x_{k1}) < \mathrm{wt}(x_{kj}) \qquad \text{für alle } j > 1.$$

Damit haben wir eine Lösung, die Standardtafel, für das Fehlerkorrekturproblem gefunden. Aber sie löst das Problem sehr ineffizient.
Was ist das wirklich?

- Die Zeilen der Standardtafel sind die Nebenklassen modulo C.
- 1. Element der Zeile: Element geringsten Gewichts aus der Nebenklasse („coset leader“).

Wenn also ein Element empfangen wird, suche die „richtige“ Nebenklasse.

$$x + C = y + C \Leftrightarrow x - y \in C \Leftrightarrow M(x - y) = 0 \Leftrightarrow Mx = My.$$

Gegeben: Linearer Code C durch Prüfmatrix M, $x \in \mathbb{F}_q^n$.

Gesucht: $c \in C$ mit $\mathrm{d}(x, c)$ minimal.

Algorithmus:

Bestimme für jede Nebenklasse ein Element x_j kleinsten Gewichts, setze $h_j = Mx_j$ („Hash-Wert“).

Suche j mit $Mx = h_j$. Gib $x - x_j$ zurück.

Abbildung 3.1: Fehlerprozessor

Korrektheit: siehe oben.
Wie kommt man nun zu den coset leaders? Die coset leaders sind genau die korrigierten Fehler.

Beispiel. • Betrachte *abcxyz*. Coset leaders:

$$7 \text{ Zeilen} \begin{cases} 000000 \\ 100000 \\ \vdots \\ 000001 \end{cases}$$

Es gilt $\dim C = 3$, $n = 6$,

$$\dim(\mathbb{F}_2^n / C) = 6 - 3 = 3.$$

8 Nebenklassen. Schreibe Stelle des 8. coset-leaders aus (2-Bit-Fehler, nicht eindeutig).
„Code hat noch etwas Luft“.

- Sei C ein binärer linearer (4,2)-Code mit Generatormatrix G und Prüfmatrix M:

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \qquad M = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Wir bekommen folgende Tabelle der cosets:

Nachrichten	00	10	01	11	
Code-Wörter	0000	1010	0111	1101	$\begin{pmatrix}0\\0\end{pmatrix}$
	1000	0010	1111	0101	$\begin{pmatrix}1\\0\end{pmatrix}$
Cosets	0100	1110	0011	1001	$\begin{pmatrix}1\\1\end{pmatrix}$
	0001	1011	0110	1100	$\begin{pmatrix}0\\1\end{pmatrix}$

Proposition 3.8. *Ein linearer Code C hat genau dann Minimaldistanz $\geq d+1$, wenn je d Spalten der Prüfmatrix M linear unabhängig sind.*

Beweis. Angenommen es gibt d linear abhängige Spalten in M. Dann gilt $M\mathbf{c} = \mathbf{0}$ und $\mathrm{wt}(\mathbf{c}) \leq d$ für ein passendes $\mathbf{0} \neq \mathbf{c} \in C$. Damit gilt $\mathrm{d}_C \leq d$.
Andererseits seien nun je d Spalten linear unabhängig, dann gibt es kein $\mathbf{0} \neq \mathbf{c} \in C$ mit $\mathrm{wt}(\mathbf{c}) \leq d$. Daraus folgt nun $\mathrm{d}_C \geq d+1$. □

Korollar 3.9. *Ein binärer linearer Code korrigiert 1-Bit Fehler genau dann, wenn alle Spalten der Prüfmatrix verschieden sind.*

Beweis. 1-Bit Fehler $\Leftrightarrow \mathrm{d}(C) \geq 3 \Leftrightarrow$ je zwei Spalten linear unabhängig über $\mathbb{F}_2 \Leftrightarrow$ je zwei Spalten verschieden. □

3.4 Hamming Codes

Definition. Sei $k \in \mathbb{N}$. Definiere den k-ten Hammincode Hamming(k) durch die Prüfmatrix $M \in \mathbb{F}_2^{k \times (2^k - 1)}$ in deren Spalten alle Vektoren aus dem $\mathbb{F}_2^k \setminus \{(0, \ldots, 0)^t\}$ stehen.

Beispiel.

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$\mathrm{rang}(M) = 3$ (Einheitsmatrix), $\dim \mathrm{Ker}\, M = 4$
Blocklänge 7, 3 Checkbits, 4 Nutzdatenbits und korrigiere 1-Bit Fehler $\Rightarrow$ Hamming(3) ist ein linearer $(7,4)$-Code, der 1-Bit Fehler korrigiert.

Satz 3.10. *Der Hammingcode Hamming(k) ist ein linearer $(2^k - 1, 2^k - k - 1)$-Code mit Minimaldistanz 3. D.h. 1-Bit Fehler können korrigiert werden.*

Beweis. Der Rang der Prüfmatrix M ist k, da die Spalten von I_k in den Spalten von M enthalten sind.

$$\dim C = \dim \mathrm{Ker}\, M = 2^k - k - 1.$$

Die Aussage über 1-Bit Fehler folgt aus dem letzten Korollar. □

Die Rate eines Hammingcodes ist gleich $\frac{2^k - k - 1}{2^k} \to^{k \to \infty} 1$. Also haben Hammingcodes eine tolle Rate aber für großes k eine lausige Fehlerkorrektur.

Definition. Ein (n, m)-Blockcode heißt r-perfekt, wenn für jedes $w \in A^k$ genau ein $v \in C$ existiert, sodass $d(v, w) \leq r$ $(r \in \mathbb{N})$.

Beispiel. *abcxyz* ist kein 1-perfekter Code, weil wir für $w = 110000$ die beiden Codewörter 110001 oder 111000 haben. Wir haben somit für $r \geq 2$ erst recht keine Eindeutigkeit.

Proposition 3.11. *Hamming(k) ist 1-perfekt.*

Beweis. Sei $w \in A^n$. $Mw = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$ für passendes $b_1, \ldots, b_k$.

$$w \in C \Leftrightarrow \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

sonst coset leaders (da alle 1-Bit Fehler korrigiert werden)

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

$\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$ kommt aber in M als Spalte vor. D.h. es existiert ein eindeutiges $j \in \{1, \ldots, k\}$ mit

$$\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} = Me_j.$$

□

Bemerkung. Es gibt ziemlich wenige perfekte Codes:

- Hammingcodes
- gewisse Wiederholungscodes
- Golay-Codes (2 Stück)

3.5 Der Satz von Shannon

Bevor wir den Satz von Shannon beweisen, wollen wir ihn mit dem folgenden Experiment motivieren. Nehmen wir an, wir befinden uns in einem Raum, in dem jemand eine Münze t mal in der Minute wirft. Dieser Raum ist mit einem zweiten Raum über ein Kabel verbunden. Über dieses Kabel können wir jeden Ausgang eines Wurfs als 0 oder 1 übertragen. Nachdem Rauschen auf dem Kanal liegt, kommt das Signal mit Wahrscheinlichkeit p falsch an, also wird mit Wahrscheinlichkeit p aus einer 0 eine 1 und umgekehrt. Einen derartigen Kanal nennt man binary symmetric channel, kurz BSC. Wir nehmen weiters an, dass wir $2t$ Symbole (also 0 und 1) pro Minute übertragen und dass wir den Kanal für die Zeit T, welche auch dieselbe Zeit ist, wie die Münzwürfe dauern, benutzen können. Dann ist offensichtlich, dass am Ende der Übertragung ein Teil p der Übertragungen fehlerhaft ist.

Wenn wir nun aber die zeitliche Begrenzung T außer Acht lassen und annehmen, dass wir beliebig lange übertragen können, dann könnten wir jedes Symbol öfter, sagen wir N mal (für N ungerade) übertragen. Die Decodierung erfolgt durch Mehrheitsentscheid, das heißt, wir decodieren das Wort als 0 oder 1 je nachdem welches Symbol öfter vorkommt. Dieser Code entspricht für $N = 3$ unserem Beispiel 2. Sei nun $p = 0.001$, dann ist die Wahrscheinlichkeit, dass der Decodierer einen Fehler macht, gleich

$$\sum_{0 \le k < \frac{N}{2}} \binom{N}{k} (1-p)^k p^{N-k} < (0.07)^N.$$

Diese Wahrscheinlichkeit geht gegen 0 für N gegen unendlich.
In unserem Fall haben wir aber dennoch eine zeitliche Schranke T, die wir einhalten müssen. Der Satz von Shannon besagt nun, dass wir trotzdem einen beliebig kleinen Übertragungsfehler erreichen können.

Satz 3.12 (Shannon 1948)**.** *Sei C ein Code mit Blocklänge n und $\mathbf{c}_1, \dots, \mathbf{c}_M$ seien die Codewörter. Sei P_i die Wahrscheinlichkeit, dass eine falsche Entscheidung getroffen wird, wenn das Codewort $\mathbf{c}_i$ übertragen wird. Dann ist die Wahrscheinlichkeit einer falschen Entscheidung für den Code gleich*

$$P_C := \frac{1}{M} \sum_{i=1}^{M} P_i.$$

Wenn $0 < R < 1 + p \log p + q \log q$ und $M_n := 2^{\lfloor Rn \rfloor}$, dann

$$\min P_C \to 0 \quad \textit{für} \quad n \to \infty,$$

wobei das Minimum über alle Codes mit Blocklänge n, Fehlerwahrscheinlichkeit p und Kardinalität M_n geht.

Wenn wir diesen Satz mit unserem Experiment vergleichen erhalten wir, dass wir für n genügend groß immer einen Code der Länge n finden, mit einer Rate nahe bei 1 (vorausgesetzt T ist große genug, sodass wir Codewörter der Länge n überhaupt übertragen können).

Beweis von Satz 3.12. Die Anzahl der Fehler in einem empfangenen Wort ist einen Zufallsvariable mit Erwartungswert np und Varianz $np(1-p)$. Wir setzen b gleich

$$b := \sqrt{\frac{np(1-p)}{(\varepsilon/2)}}.$$

Dann erhalten wir mittels Tschebyschow-Ungleichung, dass

$$P(w > np + b) \le \frac{\varepsilon}{2}. \tag{1}$$

Nachdem $p < \frac{1}{2}$ ist, ist

$$\rho := \lfloor np + b \rfloor < \frac{1}{2} n$$

für genügend großes n.
Nun definieren wir zwei Funktionen definieren, die es uns ermöglichen den Satz umzuschreiben. Konkret, seien $\mathbf{u}, \mathbf{v} \in \{0,1\}^n$, dann ist

$$f(\mathbf{u}, \mathbf{v}) = \begin{cases} 0, & \text{if } \mathrm{d}(\mathbf{u}, \mathbf{v}) > \rho, \\ 1, & \text{if } \mathrm{d}(\mathbf{u}, \mathbf{v}) \le \rho. \end{cases}$$

Für $\mathbf{c}_i \in C$ und $\mathbf{r} \in \{0,1\}^n$ sei

$$g_i(\mathbf{r}) := 1 - f(\mathbf{r}, \mathbf{c}_i) + \sum_{j \ne i} f(\mathbf{r}, \mathbf{c}_j).$$

Wenn wir nun $\mathbf{r}$ empfangen und $\mathbf{c}_i$ ist das einzige Codewort mit $\mathrm{d}(\mathbf{r},\mathbf{c}_i) \leq \rho$, dann ist $g_i(\mathbf{r}) = 0$ und sonst ist $g_i(\mathbf{r}) \geq 1$.
Wir wollen den Code nun wie folgt decodieren. Wenn wir $\mathbf{r}$ empfangen und $\mathbf{c}_i$ ist das einzige Codewort mit $\mathrm{d}(\mathbf{r},\mathbf{c}_i) \leq \rho$, dann decodieren wir $\mathbf{r}$ mit $\mathbf{c}_i$ und sonst geben wir einen Fehler zurück beziehungsweise, wenn wir decodieren müssen, geben wir $\mathbf{c}_1$ zurück.
Sei nun P_i die im Satz definierte Wahrscheinlichkeit, dass wir einen Fehler machen, wenn $\mathbf{c}_i$ übertragen wird. Dann gilt

$$P_i = \sum_{\mathbf{r}\in\{0,1\}^n} P(\mathbf{r}|\mathbf{c}_i) g_i(\mathbf{r}) = \sum_{\mathbf{r}\in\{0,1\}^n} P(\mathbf{r}|\mathbf{c}_i)\left(1 - f(\mathbf{r},\mathbf{c}_i)\right)) + \sum_{\mathbf{r}\in\{0,1\}^n} \sum_{j\neq i} P(\mathbf{r}|\mathbf{c}_i) f(\mathbf{r},\mathbf{c}_j).$$

Der erste Term auf der rechten Seite entspricht der Wahrscheinlichkeit, dass das empfangene Wort $\mathbf{r}$ einen Abstand größer ρ von $\mathbf{c}_i$ hat. Diese ist laut (1) kleiner oder gleich $\frac{1}{2}\varepsilon$. Damit erhalten wir für die Fehlerwahrscheinlichkeit des Codes

$$P_C \leq \frac{1}{2}\varepsilon + \frac{1}{M}\sum_{i=1}^{M} \sum_{\mathbf{r}\in\{0,1\}^n} \sum_{j\neq i} P(\mathbf{r}|\mathbf{c}_i) f(\mathbf{r},\mathbf{c}_j).$$

Die Hauptidee des Beweises ist es, dass das Minimum über alle Codes sicher kleiner gleich dem Erwartungswert ist. Damit erhalten wir, dass

$$\begin{aligned}
\min_C P_C &\leq \frac{1}{2}\varepsilon + \frac{1}{M}\sum_{i=1}^{M} \sum_{\mathbf{r}\in\{0,1\}^n} \sum_{j\neq i} \mathbb{E}(P(\mathbf{r}|\mathbf{c}_i))\mathbb{E}(f(\mathbf{r},\mathbf{c}_j)) \\
&\leq \frac{1}{2}\varepsilon + \frac{1}{M}\sum_{i=1}^{M} \sum_{\mathbf{r}\in\{0,1\}^n} \sum_{j\neq i} \mathbb{E}(P(\mathbf{r}|\mathbf{c}_i))\frac{|B(\mathbf{c}_j,\rho)|}{2^n} \\
&\leq \frac{1}{2}\varepsilon + (M-1)2^{-n}|B(\mathbf{c}_j,\rho)|,
\end{aligned}$$

wobei

$$B(\mathbf{x},\rho) := \{\mathbf{y} \in \{0,1\}^n : \mathrm{d}(\mathbf{x},\mathbf{y}) \leq \rho\}.$$

Wir erhalten mit der Stirling'schen Formel als Abschätzung für die Elemente in einer Kugel vom Radius ρ

$$|B(\mathbf{x},\rho)| = \sum_{k=0}^{\rho} \binom{n}{k} < \frac{1}{2} n \binom{n}{\rho} \leq \frac{1}{2} n \frac{n^n}{\rho^\rho (n-\rho)^{n-\rho}}.$$

Davon nehmen wir den Logarithmus und erhalten

$$\begin{aligned}
\log|B(\mathbf{x},\rho)| &< -1 + \log n + n\log n - \rho\log\rho - (n-\rho)\log(n-\rho) \\
&= -1 + \log n - \rho\log\frac{\rho}{n} - (n-\rho)\log\left(1-\frac{\rho}{n}\right).
\end{aligned}$$

Wir setzen ein und dividieren durch n

$$\frac{1}{n}\log\left(\min_C P_C - \frac{1}{2}\varepsilon\right) \leq \frac{1}{n}\log M - \left(1 - \frac{\log n}{n} + \frac{\rho}{n}\log\frac{\rho}{n} + \left(1-\frac{\rho}{n}\right)\log\left(1-\frac{\rho}{n}\right)\right).$$

Nun stürzen wir uns auf die Klammer rechts und schätzen die beiden letzten Terme ab. Wir erhalten

$$\frac{\rho}{n}\log\frac{\rho}{n} = \frac{1}{n}\lfloor np+b\rfloor \log\frac{\lfloor np+b\rfloor}{n} = p\log p + \mathcal{O}(n^{-\frac{1}{2}})$$

und

$$\left(1-\frac{\rho}{n}\right)\log\left(1-\frac{\rho}{n}\right) = (1-p)\log(1-p) + \mathcal{O}(n^{-\frac{1}{2}}).$$

Eingesetzt ergibt dies

$$\frac{1}{n}\log\left(\min_C P_C - \frac{1}{2}\varepsilon\right) \leq \frac{1}{n}\log M - (1 + p\log p + (1-p)\log(1-p)) + \mathcal{O}(n^{-\frac{1}{2}}).$$

Wir ersetzen M mit M_n und erhalten mit den Schranken für R, dass

$$\frac{1}{n}\log\left(\min_C P_C - \frac{1}{2}\varepsilon\right) < -\beta < 0$$

für genügend großes n und somit $\min_C P_C < \frac{1}{2}\varepsilon + 2^{-\beta n}$. □

Kapitel 4

BCH Codes und andere polynomielle Codes

4.1 BCH Codes als Subcodes von Hammingcodes

Nachdem wir im vorigen gezeigt haben, dass ein Hammingcode perfekt ist, wollen wir diesen nun als Ausgangspunkt für einen Code wählen, der mehr als einen Fehler korrigiert, indem wir zusätzliche Zeilen in die Prüfmatrix schreiben. Damit wir überhaupt etwas erreichen, dürfen neue Zeilen nicht als Linearkombination alter Zeilen entstehen. Trotzdem sollten wir die neuen Zeilen nicht willkürlich wählen, sondern dem Ganzen eine Systematik zu Grunde legen, damit die spätere Analyse leichter wird. Eine erste Idee ist es, die neuen Zeilen als Polynome in den alten Zeilen zu erzeugen. Wir müssen aber bedenken, dass es auch zu trivialen „Erweiterungen" kommen kann. So sind die Polynomfunktionen über $\mathbb{F}_2$ uninteressant, denn

$$x^k = x \quad \text{für alle } x \in \mathbb{F}_2 \text{ und } k \in \mathbb{N}.$$

Beispiel. Wir betrachten den Hamming(3) etwas näher.

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Jede Spalte entspricht eindeutig einem $0 \neq \beta \in \mathbb{F}_8 \asymp \mathbb{F}_2[X]/(X^3 + X^2 + 1)$, denn

$$\begin{pmatrix} b_2 \\ b_1 \\ b_0 \end{pmatrix} \leftrightarrow b_0 + b_1 X + b_2 X^2 \in \mathbb{F}_2[X]/(X^3 + X^2 + 1).$$

Die Prüfmatrix entspricht

$$\begin{pmatrix} X^6 & X^5 & X^4 & X^3 & X^2 & X & 1 \\ X^{12} & X^{10} & X^8 & X^6 & X^4 & X^2 & 1 \\ X^{18} & X^{15} & X^{12} & X^9 & X^6 & X^3 & 1 \\ X^{24} & X^{20} & X^{16} & X^{12} & X^8 & X^4 & 1 \end{pmatrix}$$

Nachdem die Determinanten aller 4x4-Untermatrizen nicht 0 sind ist die Minimaldistanz gleich 5 und somit sind 2 Fehler korrigierbar.

Definition. Sei p eine Primzahl, $k, t \in \mathbb{N}$ und β ein primitives Element von $\mathbb{F}_{p^k}$. Sie Ψ die Koordinatenabbildung, d.h.

$$\begin{array}{lccc} \Psi: & \mathbb{F}_p^k & \to & \mathbb{F}_{p^k} \\ & (d_0, \ldots, d_{k-1})^t & \mapsto & \sum_{j=0} d_j \beta^j. \end{array}$$

Der lineare Code mit Prüfmatrix

$$\begin{pmatrix} \Psi^{-1}(\beta^{p^k-1}) & \dots & \Psi^{-1}(\beta) & \Psi^{-1}(1) \\ \Psi^{-1}(\beta^{2p^k-1}) & \dots & \Psi^{-1}(\beta^2) & \Psi^{-1}(1^2) \\ \vdots & & \vdots & \vdots \\ \Psi^{-1}(\beta^{2t(p^k-1)}) & \dots & \Psi^{-1}(\beta^{2t}) & \Psi^{-1}(1^{2t}) \end{pmatrix}$$

heißt BCH(k,t)-Code über $\mathbb{F}_p$.

Dieser Code ist nach seinen Erfindern R.C. Bose, D.K. Ray-Chaudhuri und A. Hocquenghem benannt.

Satz 4.1. *Der BCH(k,t) ist ein linearer Code über $\mathbb{F}_p$ mit Blocklänge $n = p^k - 1$ und Minimaldistanz $\geq 2t+1$ (d.h. t Fehler können korrigiert werden).*

Beweis. Nachdem die Prüfmatrix $p^k - 1$ Spalten hat, ist die Blocklänge $p^k - 1$. Es bleibt zu zeigen, dass die Minimaldistanz $\geq 2t+1$ ist. Dies ist genau dann der Fall, wenn je $2t$ Spalten der Prüfmatrix linear unabhängig über $\mathbb{F}_p$ sind. Wir wählen also $2t$ Spalten

$$\begin{pmatrix} \Psi^{-1}(\beta^{j_i}) \\ \Psi^{-1}(\beta^{2j_i}) \\ \vdots \\ \Psi^{-1}(\beta^{2tj_i}) \end{pmatrix} \quad \text{für } 0 \leq j_1 \leq \dots \leq j_{2t} \leq p^k - 2.$$

Diese $2t$ Spalten sind linear unabhängig über $\mathbb{F}_p$

$$\iff \begin{pmatrix} \beta^{j_i} \\ \beta^{2j_i} \\ \vdots \\ \beta^{2tj_i} \end{pmatrix} \quad \text{für } 0 \leq j_1 \leq \dots \leq j_{2t} \leq p^k - 2 \text{ linear unabhängig über } \mathbb{F}_p \text{ sind.}$$

$$\impliedby \begin{pmatrix} \beta^{j_i} \\ \beta^{2j_i} \\ \vdots \\ \beta^{2tj_i} \end{pmatrix} \quad \text{für } 0 \leq j_1 \leq \dots \leq j_{2t} \leq p^k - 2 \text{ linear unabhängig über } \mathbb{F}_{p^k} \text{ sind.}$$

$$\iff \begin{pmatrix} \beta^{j_{2t}} & \dots & \beta^{j_1} \\ \vdots & & \vdots \\ \beta^{2tj_{2t}} & \dots & \beta^{2tj_1} \end{pmatrix} \quad \text{eine reguläre Matrix über } \mathbb{F}_{p^k} \text{ ist.}$$

$$\iff \det \begin{pmatrix} \beta^{j_{2t}} & \dots & \beta^{j_1} \\ \vdots & & \vdots \\ \beta^{2tj_{2t}} & \dots & \beta^{2tj_1} \end{pmatrix} \neq 0.$$

Nun ist aber die Determinate gleich

$$\begin{aligned} \det \begin{pmatrix} \beta^{j_{2t}} & \dots & \beta^{j_1} \\ \vdots & & \vdots \\ \beta^{2tj_{2t}} & \dots & \beta^{2tj_1} \end{pmatrix} &= \beta^{j_{2t}} \beta^{j_{2t-1}} \cdots \beta^{j_1} \cdot \det \begin{pmatrix} 1 & \dots & 1 \\ \beta^{j_{2t}} & \dots & \beta^{j_1} \\ \vdots & & \vdots \\ (\beta^{j_{2t}})^{2t-1} & \dots & (\beta^{j_1})^{2t-1} \end{pmatrix} \\ &= \beta^{j_{2t}} \beta^{j_{2t-1}} \cdots \beta^{j_1} \prod_{1 \leq i < j \leq 2t} (\beta^{j_i} - \beta^{j_j}) \neq 0. \end{aligned}$$

□

Im Beweis des vorigen Satzes haben wir die exakte Darstellung der Determinante der Vandermonde-Matrix benötigt, die wir nun beweisen wollen.

Lemma 4.2. *Sei R ein ZPE-Ring und $X_1, \ldots, X_n$ Unbestimmte über R. Dann gilt*

$$\det \begin{pmatrix} 1 & \cdots & 1 \\ X_1 & \cdots & X_n \\ \vdots & & \vdots \\ X_1^{n-1} & \cdots & X_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (X_j - X_i) \neq 0.$$

Beweis. Sie $P(X_1, \ldots, X_n) = \det(\cdot)$ das charakteristische Polynom. Dann ist der Totalgrad des Polynoms

$$\deg P \le (n-1) + (n-2) + \cdots + 1 + 0 = \frac{(n-1)n}{2}.$$

Wenn nun $X_i = X_j$, dann sind zwei Spalten gleich und somit die Determinante 0. Also

$$(X_i - X_j) \mid P(X_1, \ldots, X_n) \text{ für } 1 \le i < j \le n.$$

Da alle $(X_i - X_j)$ mit $1 \le i < j \le n$ relativ prim sind, gilt auch

$$\prod_{1 \le i < j \le n} (X_i - X_j) \mid P(X_1, \ldots, X_n).$$

Für den Totalgrad des Produktes auf der linken Seite ergibt sich

$$\deg \prod_{1 \le i < j \le n} (X_i - X_j) = \binom{n}{2} = \frac{n(n-1)}{2}.$$

Damit sind die Grade gleich und die linke und rechte Seite kann sich nur um eine Konstante unterscheiden. Also

$$P(X_1, \ldots, X_n) = C \cdot \prod_{1 \le i < j \le n} (X_i - X_j).$$

Wir vergleichen den Koeffizienten bei $X_n^{n-1} X_{n-1}^{n-2} \cdots X_2^1 X_1^0$. Dies ist das Leitmonom bezüglich der Ordnung $X_n > X_{n-1} > \cdots > X_2 > X_1$. Wir erhalten

- in $P(X_1, \ldots, X_n)$ den Koeffizient 1,
- in $\prod_{1 \le i < j \le n} (X_i - X_j)$ den Koeffizient 1.

Damit muss $C = 1$ sein und wir sind fertig. □

Proposition 4.3 (Redundanz in der Prüfmatrix)**.** *Jede p-te Zeile, d.h. die Zeilen der Gestalt*

$$\left(\Psi^{-1}(\beta^{ipj})_j\right),$$

können aus der Prüfmatrix eines BCH-Codes weggelassen werden, ohne, dass sich der Code ändert.

Beweisskizze. Die Abbildung $\Phi_p : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}, x \mapsto x^p$ (Frobenius-Automorphismus) ist eine $\mathbb{F}_p$ lineare Abbildung. Die ip-te Zeile der Prüfmatrix entsteht also linear aus der i-ten Zeile, ist also überflüssig. □

Im Spezialfall $p = 2$ ist also nur jede 2-te Zeile interessant.

4.2 Polynomielle Codes unter besonderer Berücksichtigung von BCH-Codes

Die (volle) Prüfmatrix eines BCH-Codes war

$$\begin{pmatrix} \beta^{p^k-1} & \dots & \beta & 1 \\ \beta^{2p^k-1} & \dots & \beta^2 & 1^2 \\ \vdots & & \vdots & \vdots \\ \beta^{2t(p^k-1)} & \dots & \beta^{2t} & 1^{2t} \end{pmatrix}$$

Sei also $\mathbf{c} = (c_{n-1}, \dots, c_0) \in \mathbb{F}_p^n$, dann ist

$$\begin{aligned} \mathbf{c} \in \text{Code} &\iff \sum_{j=0}^{n-1} c_j (\beta^i)^j = 0 \text{ für } 1 \le i \le 2t \\ &\iff \tilde{c}(\beta^i) = 0 \text{ für } \tilde{c} := \sum_{j=0}^{n-1} c_j X^j \text{ für } 1 \le i \le 2t. \end{aligned}$$

Proposition 4.4. *Betrachte BCH(k,t)-Code mit primitivem Element $\beta \in \mathbb{F}_{p^k}$. Sei g_i das Minimalpolynom von $\beta^i \in \mathbb{F}_{p^k}$ über $\mathbb{F}_p$. Sei g das Produkt der verschiedenen g_i, d.h.*

$$g := \prod_{i=1}^{2t} g_i.$$

Dann gilt

$$\mathbf{c} = (c_{n-1}, \dots, c_0)^t \in \text{BCH}(k,t) \iff g \mid \sum_{j=0}^{n-1} c_j X^j.$$

Beweis.

$$\begin{aligned} \mathbf{c} \in \text{BCH}(k,t) &\iff \tilde{c}(\beta^i) = 0 \text{ für } 1 \le i \le 2t \\ &\iff g_i \mid \tilde{c} \text{ für alle } 1 \le i \le 2t \\ &\iff \text{kgV}(\{g_i : i = 1, \dots, 2t\}) \mid \tilde{c}. \end{aligned}$$

Da jedes g_i irreduzibel und normiert ist, gilt

$$\text{kgV}(g_i, g_j) = \begin{cases} g_i & g_i = g_j, \\ g_i g_j & g_i \neq g_j. \end{cases}$$

Also folgt $\text{kgV}(\{g_i : i = 1, \dots, 2t\}) = g$. □

Beweis von Proposition 4.3.

$$\begin{aligned} \tilde{c}(\beta^{ip}) &= (\tilde{c}(\beta^i)^p, \\ 0 &= 0. \end{aligned}$$

□

Bemerkung. Wir treffen folgende Konvention:

$$(c_{n-1}, \dots, c_0) \in \mathbb{F}_p^n \longleftrightarrow \sum_{j=0}^{n-1} c_j X^j \in \mathbb{F}_p[X]$$

Definition. Sei p eine Primzahl und $n \in \mathbb{N}$. Ein linearer Code $C \trianglelefteq \mathbb{F}_p^n$ heißt Polynomialer Code, wenn es ein $g \in \mathbb{F}_p[X]$ gibt, mit

$$C = \{c \in \mathbb{F}_p^n : g \mid c\}.$$

Bemerkung.
- Obige Proposition zeigt, dass der BCH(k,t) ein Polynomialer Code ist.
- g heißt das Generatorpolynom.

Definition. Wir definieren die Linksrotation als

$$\mathrm{rot} : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p^n, \quad (c_{n-1}, \ldots, c_0) \mapsto (c_{n-2}, \ldots, c_1, c_0, c_{n-1}).$$

Satz 4.5 (Charakterisierung von Polynomiellen Codes)**.** *Sei $C \trianglelefteq \mathbb{F}_p^n$ ein linearer Code. Dann sind die folgenden Aussagen äquivalent:*

1. *C ist polynomieller Code.*
2. *$\mathrm{rot}(0, c_{n-2}, \ldots, c_0) \in C$, falls $(0, c_{n-2}, \ldots, c_0) \in C$.*

Beweis.
- (1)⇒(2): Sei $C = \{c \in \mathbb{F}_p^n : g \mid c\}$ und sei $\mathbf{c} = (0, c_{n-2}, \ldots, c_0) \in C$. Also gibt es ein $h \in \mathbb{F}_p[X]$ mit $c = g \cdot h$ und $\deg h \leq n - 2 - \deg g$. Es folgt, dass

  $$\mathrm{rot}(\mathbf{c}) = X \cdot \mathbf{c} + 0 = X \cdot \mathbf{c} = g(X \cdot h).$$

  Da nun $\deg(g(X \cdot h)) \leq \deg(g) + 1 + n - 2 - \deg(g) = n - 1$ und $g \mid \mathrm{rot}(\mathbf{c})$, gilt $\mathrm{rot}(\mathbf{c}) = g(X \cdot h) \in C$.
- (2)⇒(1): Wähle $g \in C$ so, dass g minimalen Grad aller von 0 verschiedenen Codewörter (Codepolynome) hat. Setze $d := \deg g$. Dann ist $g = (0, \ldots, 0, g_d, \ldots, g_0) \in C$. Es folgt, dass $gX = \mathrm{rot}(g) \in C$ und durch Iteration auch $gX^k = \mathrm{rot}^k(g) \in C$ für $1 \leq k \leq n - d - 1$. Setze

  $$\tilde{C} := \{c \in \mathbb{F}_p^n : g \mid c\} = \mathrm{span}\{g, Xg, \ldots, X^{n-d-1}g\}.$$

  Da $c = g \cdot h$ mit $\deg h \leq n - d - 1$, folgt, dass $h \in \mathrm{span}\{1, X, \ldots, X^{n-d-1}\}$ und somit dass $\tilde{C} \trianglelefteq C$.

  Sei nun $c \in C \setminus \tilde{C}$. Dann gibt es mittels Division mit Rest Polynome $q, r \in \mathbb{F}_p[X]$ mit $c = qp + r$, wobei $\deg r < \deg g = d$. Nun ist aber $c \in C$ und $q \cdot g \in \tilde{C} \subset C$, womit $r \in C$ folgt. Nachdem aber $\deg r < \deg g$ ist, folgt ein Widerspruch zur Wahl von g. Damit gilt $\tilde{C} = C$.

□

Proposition 4.6. *Sei C ein polynomieller Code, $C \trianglelefteq \mathbb{F}_p^n$, mit Generatorpolynom g. Dann gilt*

$$E : \mathbb{F}_p^{n-1-\deg g} \longrightarrow \mathbb{F}_p^n, \quad h \mapsto g \cdot h$$

ist ein Codierer für C. Insbesondere gilt, dass $\dim C = n - 1 - \deg g$.

Bemerkung. Es handelt sich also um einen systematischen Codierer.

Beweis der Proposition. Nach dem Beweis von Satz 4.5 gilt

$$C = \{c \in \mathbb{F}_p^n : \deg c \leq n - 1, g \mid c\} = \mathrm{span}\{g, \ldots, X^{n-\deg g-1}g\}$$

und alles folgt. □

Bemerkung. Sei C ein polynomieller Code, mit Generatorpolynom g, also $C = \{g \cdot h : \deg h \leq n - 1 - \deg g\}$, dann kann jedenfalls durch Division durch g mit Rest decodiert werden.

Definition. Ein Code C heißt zyklisch, wenn $\forall c \in C : \mathrm{rot}\, c \in C$ (d.h. zyklische Permutationen führen C in C über).

Laut Satz 4.5 ist jeder zyklische lineare Code ein polynomieller Code. Wie übersetzt sich die Bedingung zyklisch auf das Generatorpolynom?

Satz 4.7 (Charakterisierung von zyklischen Codes)**.** *Sei C ein linearer Code aus $\mathbb{F}_q^n$ (q eine Primzahlpotenz). Dann sind folgende Aussagen äquivalent:*

1. *C ist ein zyklischer Code.*
2. *C ist ein polynomieller Code mit Generatorpolynom g, sodass $g \mid X^n - 1$.*

Beweis.

- (1)⇒(2): Sei C zyklisch, dann ist C laut Satz 4.5 ein polynomieller Code. Sei g sein Generatorpolynom und g sei oBdA normiert. Dann gilt offensichtlich $X^{n-1-\deg g} \cdot g \in C$. Wir können g nun schreiben als

$$g = \sum_{j=0}^{d} g_j X^j \longleftrightarrow (0, \ldots, 0, 1, g_{d-1}, \ldots, g_0).$$

  Damit folgt für

$$X^{n-1-\deg g} g \longleftrightarrow (1, g_{d-1}, \ldots, g_0).$$

  Für die Linksrotation ergibt sich somit,

$$\mathrm{rot}(X^{n-1-\deg g} g) = X^{n-1-\deg g} g X - X^n + 1 = X^{n-\deg g} g - (X^n - 1).$$

  Schließlich folgt aus

$$\begin{aligned} \mathrm{rot}(X^{n-1-\deg g} g) \in C &\Rightarrow g \mid \mathrm{rot}(X^{n-1-\deg g} g) = X^{n-\deg g} g - (X^n - 1) \\ &\Rightarrow g \mid (X^n - 1). \end{aligned}$$

- (2)⇒(1): Sei $c \in C$ mit $c = (c_{n-1}, \ldots, c_0)$. Dann gilt für die Linksrotation

$$\mathrm{rot}(c) = X \cdot c - c_n X^n + c_n = X \cdot c \cdot c_n (X^n - 1).$$

  Da nun $g \mid c$ und $g \mid (X^n - 1)$ folgt, dass $g \mid \mathrm{rot}\, c$.

□

Für den BCH-Code können wir damit folgendes beweisen.

Satz 4.8. *Jeder BCH-Code ist zyklisch.*

Beweis. Sei g das Produkt verschiedener irreduzibler Polynome g_j, wobei g_j das Minimalpolynom von β^j war mit $\beta \in \mathbb{F}_{p^k}$. Wir wissen, dass $\beta^{j(p^k-1)} = 1$. Damit folgt, dass $g_j \mid X^{p^k-1} - 1$. Nachdem $n = p^k - 1$, folgt, dass

$$g_j \mid X^n - 1 \Longrightarrow g = \mathrm{kgV}(g_j) \mid X^n - 1.$$

□

Wir wollen uns nun näher damit beschäftigen, wie man zyklische Codes decodiert.

Satz 4.9 (Decodierer von zyklischen Codes)**.** *Sei $g \in \mathbb{F}_q[X]$ mit $g \mid X^n - 1$ und $h := \frac{X^n-1}{g} \in \mathbb{F}_q[X]$. Sei weiters C der polynomieller Code mit Generatorpolynom g, also*

$$C = \{g \cdot f : \deg f \leq n - 1 - \deg g\}.$$

Schließlich sei $c \in \mathbb{F}_q[X]$ mit $\deg c \leq n - 1$. Dann gilt

$$c \in C \Longleftrightarrow c \cdot h \leftrightarrow (a_{n-1}, \ldots, a_0, -a_{n-1}, \ldots, -a_0),$$

wobei führende Nullen erlaubt sind. In diesem Fall gilt:

$$\frac{c}{g} \leftrightarrow (a_{n-1}, \ldots, a_0).$$

Proof. Sei $c = g \cdot f + r$ mit $\deg r < \deg g$. Dann folgt

$$c \cdot h = g \cdot h \cdot f + r \cdot h = (X^n - 1)f + r \cdot h.$$

Sei nun $f \leftrightarrow (a_{n-1}, \ldots, a_0)$, dann gilt, dass

$$(X^n - 1)f \leftrightarrow (a_{n-1}, \ldots, a_0, 0, \ldots, 0) - (0, \ldots, 0, a_{n-1}, \ldots, a_0) = (a_{n-1}, \ldots, a_0, -a_{n-1}, \ldots, -a_0).$$

Nun sei $r \cdot h \leftrightarrow (b_{n-1}, \ldots, b_0)$ und es folgt, dass

$$c \cdot h \leftrightarrow (a_{n-1}, \ldots, a_0, -a_{n-1} + b_{n-1}, \ldots, -a_0 + b_0).$$

Wir haben noch nicht verwendet, dass $c \in C$ ist. Also gilt

$$c \in C \Leftrightarrow r = 0 \Leftrightarrow r \cdot h = 0 \Leftrightarrow c \cdot h = (a_{n-1}, \ldots, a_0, -a_{n-1}, \ldots, -a_0).$$

□

Damit ist das Decodieren eines zyklischen Codes durch weitere Multiplikation mit dem richtigen Polynom und anschließendem Vergleich des vorderen und hinteren Anteils zu bewerkstelligen. Wir müssen beachten, dass in Charakteristik 2 die Vorzeichen verschwinden.

Systematische Codierung

Gegeben: $f \in \mathbb{F}_q[X]$, $\deg f \leq n - 1 - \deg g$, $f \leftrightarrow (f_m, \ldots, f_0)$.

Gesucht: $r \in \mathbb{F}_q[X]$ mit $r \leftrightarrow (r_{\deg g - 1}, \ldots, r_0)$,
sodass $(f_m, \ldots, f_0, r_{\deg g - 1}, \ldots, r_0) \in C$.

Algorithmus: Es gilt $m = n - 1 - \deg g$. Wir suchen also

$$(f_m, \ldots, f_0, r_{\deg g - 1}, \ldots, r_0) \in C.$$

Nachdem C ein polynomieller Code ist, ist das gleichbedeutend mit

$$\begin{aligned} & X^{\deg g} f + r \equiv 0 \pmod{g}, \\ \Rightarrow\ & X^{\deg g} = Q \cdot g - r, \quad \deg r < \deg g, \\ \Rightarrow\ & \text{berechne } (-r) \text{ durch Division von } f \text{ durch } g \text{ mit Rest.} \end{aligned}$$

Bemerkung.

Vorteil: Diese Verfahren ist systematisch und macht das dekodieren somit einfach.

Nachteil: Die Polynomdivision ist nicht immer billig, aber über $\mathbb{F}_2$ auch nicht tragisch.

4.3 Effiziente Fehlerkorrektur für BCH-Codes

Wir betrachten den BCH-Code(k,t) mit der Checkmatrix

$$\left(\beta^{jr}\right)_{\substack{1 \leq j \leq 2t \\ 0 \leq r \leq q^k - 2}},$$

wobei β ein primitives Element aus dem $\mathbb{F}_q$ ist.

Lemma 4.10. *Sei* $\mathbf{c}$ *ein Codewort,* $\mathbf{e}$ *ein Fehler vom Gewicht* $s \leq t$. *Wir setzen* $\mathbf{d} = \mathbf{c} + \mathbf{e}$ *und*

$$s(z) := \sum_{j=0}^{2t-1} \tilde{d}(\beta^{j+1}) z^j.$$

Dann gibt es genau ein Tripel $(\ell(z), u(z), w(z))$ *von Polynomen über* $\mathbb{F}_q$ *mit folgenden Eigenschaften:*

- $\deg \ell \leq t$, $\ell(0) = 1$,
- $\deg u, \deg w < t$,
- $\mathrm{ggT}(\ell(z), u(z)) = 1$,
- $\ell(z) \cdot s(z) + u(z) \cdot z^{2t} = w(z)$,

nämlich

$$\begin{aligned}
\ell(z) &= \prod_{j \in M} (1 - \beta^j z), \\
u(z) &= \sum_{j \in M} e_j \beta^{2t+1} \prod_{\substack{i \neq j \\ i \in M}} (1 - \beta^i z), \\
w(z) &= \sum_{j \in M} e_j \beta^j \prod_{\substack{i \neq j \\ i \in M}} (1 - \beta^i z),
\end{aligned}$$

wobei $M = \{m \in \{0, \dots q^k - 2\} : e_m \neq 0\}$.

Bemerkung. Wenn es gelingt, $\ell(z)$, $w(z)$ über andere Methoden zu erhalten, muss nur $\ell(z)$ faktorisiert werden, um jene m zu bestimmen, wo ein Fehler aufgetreten ist. Unter Verwendung von w sind auch die e_m erhältlich.

Beweis. 1. Es gibt höchstens ein solches Tripel. Andernfalls seien (ℓ_1, u_1, w_1) und (ℓ_2, u_2, w_2) zwei solche Tripel. Dann gilt

$$\left.\begin{aligned}
\ell_1(z) \cdot s(z) + u_1(z) z^{2t} = w_1(z) \mid \cdot \ell_2 \\
\ell_2(z) \cdot s(z) + u_2(z) z^{2t} = w_2(z) \mid \cdot \ell_1
\end{aligned}\right\} -$$
$$z^{2t}(u_1 \ell_2 - \ell_1 u_2) = \ell_2 w_1 - \ell_1 w_2.$$

Nun ist aber die rechte Seite vom Grad her kleiner als 2^t und somit muss

$$\begin{aligned}
u_1 \ell_2 &= \ell_1 u_2 \quad \text{und} \\
\ell_2 w_1 &= \ell_1 w_2.
\end{aligned}$$

Da $\mathrm{ggT}(u_2, \ell_2) = 1$, folgt mit $\ell_2 \mid u_1 \ell_2 = \ell_1 u_2$, dass $\ell_2 \mid \ell_1$, und analog, dass $\ell_1 \mid \ell_2$. Somit muss $\ell_1 = f \cdot \ell_2$ mit $f \in \mathbb{F}_q$. Wegen $\ell_1(0) = \ell_2(0) = 1$ muss $f = 1$ sein und somit $\ell_1 = \ell_2$. Damit folgt aber $u_1 = u_2$ und $w_1 = w_2$.

2. Die angegebenen Polynome leisten, was von ihnen erwartet wird. Sei $\mathbf{d} = \mathbf{c} + \mathbf{e}$ und $\mathbf{c}$ ein Codewort. Dann folgt, dass

$$d(\beta^{k+1}) = c(\beta^{k+1}) + e(\beta^{k+1}) = e(\beta^{k+1}) = \sum_{j \in M} e_j \beta^{(k+1)j}.$$

Damit folgt für $s(z)$, dass

$$\begin{aligned}
s(z) &= \sum_{k=0}^{2t-1} \sum_{j \in M} e_j \beta^{(k+1)j} z^k = \sum_{j \in M} e_j \beta^j \sum_{k=0}^{2t-1} (\beta z)^k = \sum_{j \in M} e_j \beta^j \frac{1 - (\beta^j z)^{2t}}{1 - \beta^j z} \\
&= \sum_{j \in M} e_j \beta^j \frac{1}{1 - \beta^j z} - z^{2t} \sum_{j \in M} e_j \beta^{j(2t+1)} \frac{1}{1 - \beta^j z}.
\end{aligned}$$

Wenn wir nun mit dem gemeinsamen Nenner $\ell(z)$ multiplizieren erhalten wir

$$\ell(z) s(z) = w(z) - z^{2t} u(z).$$

Wir notieren uns, dass

$$\frac{w(z)}{\ell(z)} = \sum_{j \in M} e_j \beta^j \frac{1}{1 - \beta^j z}$$

ist. Damit können wir die Koeffizienten von $e_j \beta^j$ aus der Partialbruchzerlegung von $\frac{w(z)}{\ell(z)}$ ablesen. Wir wissen, dass $|M| = s \leq t$ gilt. Damit folgt

- $\deg \ell = s \leq t$,
- $\deg w \leq s - 1 < t$,
- $\deg u \leq s - 1 < t$ und
- $\ell(0) = \prod_{j \in M} (1 - 0) = 1$.

Damit bleibt noch der $\mathrm{ggT}(\ell, u)$ zu zeigen. Die Primfaktoren (irreduzible Faktoren) von ℓ sind die Polynome $1 - \beta^j z$. Nun gilt aber für $j \in M$

$$1 - \beta^j z \mid u(z) \Leftrightarrow u\left(\frac{1}{\beta^j}\right) = 0 \Leftrightarrow e_j \beta^{j(2t+1)} \prod_{\substack{i \neq j \\ i \in M}} \left(1 - \beta^{i-j}\right) = 0 \Leftrightarrow \text{ nie.}$$

Somit folgt, dass der $\mathrm{ggT}(\ell, u) = 1$ ist.

□

Wir wollen nun den erweiterten Euklidischen Algorithmus anwenden um die Polynome ℓ, u und w zu finden. Um dies zufriedenstellen durchzuführen müssen wir dem Algorithmus zuerst ein paar technische Details entlocken.

Lemma 4.11 (Euklidischer Algorithmus revised)**.** *Sei R ein euklidischer Bereich, f und $g \in R$. Wir betrachten den erweiterten Euklidischen Algorithmus und setzen hierzu*

$$\begin{gathered} h_0 = f, \quad x_0 = 1, \quad y_0 = 0, \\ h_1 = g, \quad x_1 = 0, \quad y_1 = 1, \\ h_{j-1} = h_j q_j + h_{j+1} \quad \textit{(Division mit Rest)}, \\ \begin{pmatrix} h_j & x_j & y_j \\ h_{j+1} & x_{j+1} & y_{j+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_j \end{pmatrix} \begin{pmatrix} h_{j-1} & x_{j-1} & y_{j-1} \\ h_j & x_j & y_j \end{pmatrix}. \end{gathered}$$

Dann gilt

1. $\det \begin{pmatrix} x_j & y_j \\ x_{j+1} & y_{j+1} \end{pmatrix} = \pm 1$,
2. $\det \begin{pmatrix} h_j & x_j \\ h_{j+1} & x_{j+1} \end{pmatrix} = \pm g$,
3. $\det \begin{pmatrix} h_j & y_j \\ h_{j+1} & y_{j+1} \end{pmatrix} = \pm f$,
4. $h_j = x_j \cdot f + y_j \cdot g$.

Falls $R = K[X]$ für einen Körper K, dann gelte weiters

5. $(\deg h_j)_{j \geq 1}$ *ist streng monoton fallend und*
6. $(\deg x_j)_{j \geq 2}$ *und* $(\deg y_j)_{j \geq 1}$ *sind streng monoton wachsend falls* $\deg f > \deg g$.
7. $\mathrm{ggT}(x_j, y_j) = 1$.

Beweis. 1. Nachdem

$$\begin{pmatrix} x_j & y_j \\ x_{j+1} & y_{j+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_j \end{pmatrix} \begin{pmatrix} x_{j-1} & y_{j-1} \\ x_j & y_j \end{pmatrix}$$

folgt, dass

$$\det \begin{pmatrix} x_j & y_j \\ x_{j+1} & y_{j+1} \end{pmatrix} = -\det \begin{pmatrix} x_{j-1} & y_{j-1} \\ x_j & y_j \end{pmatrix} = \cdots = \pm \det \begin{pmatrix} x_0 & y_0 \\ x_1 & y_1 \end{pmatrix} = \pm 1.$$

2. Analog wie 1., denn
$$\det \begin{pmatrix} h_0 & x_0 \\ h_1 & x_1 \end{pmatrix} = \det \begin{pmatrix} f & 1 \\ g & 0 \end{pmatrix} = -g.$$

3. Analog wie 1., denn
$$\det \begin{pmatrix} h_0 & y_0 \\ h_1 & y_1 \end{pmatrix} = \det \begin{pmatrix} f & 0 \\ g & 1 \end{pmatrix} = f.$$

4. Das ist bekannt (mehrfache Rekursion mit $(1, -f, -g)$).

5. Der Grad von h_{j+1} ist kleiner als jener von h_j, weil h_{j+1} als Rest bei Division mit Rest von h_{j-1} durch h_j auftritt.

6. Da $\deg h_j < \deg h_{j-1}$ folgt, dass $\deg q_j \geq 1$. Es gilt nun, $x_{j+1} = x_{j-1} - q_j x_j$. Damit folgt für die Grade, dass $\deg x_{j+1} = \deg x_{j-1} - q_j x_j = \deg q_j + \deg x_j > \deg x_j$, weil $\deg x_{j-1} < \deg x_j q_j$.

7. Da
$$\det \begin{pmatrix} x_j & y_j \\ x_{j+1} & y_{j+1} \end{pmatrix} = x_j y_{j+1} - x_{j+1} y_j = \pm 1$$
folgt, dass $\mathrm{ggT}(x_{j+1}, y_{j+1}) = 1$.

□

Wir können nun einen Algorithmus angeben, der das Tripel (ℓ, u, w) berechnet.

Satz 4.12. *Der Algorithmus 4.1 terminiert und ist korrekt.*

Bemerkung. Der Algorithmus 4.1 ist ziemlich effizient.

Beweis. Da $(\deg h_j)_{j \geq 0}$ streng monoton fallend ist (denn $\deg s \leq 2t-1 < \deg z^{2t} = 2t$), terminiert der Algorithmus.
Für die Korrektheit reicht es zu zeigen, dass die so berechneten Polynome ℓ, u und w den Bedingungen des Lemmas 4.10 genügen. Angenommen $y_j(0) \neq 0$. Nach Lemma 4.11 wissen wir, dass

- in jedem Schritt gilt
$$\begin{aligned} & h_j(z) = z^{2t} x_j(z) + s(z) \\ \Longrightarrow \quad & w(z) = z^{2t} u(z) + s(z)\ell(z), \end{aligned}$$
- in jedem Schritt gilt $\mathrm{ggT}(x_j, y_j) = 1$ und somit $\mathrm{ggT}(u, \ell) = 1$,
- $\ell(0) = 1$,
- $\deg w < t$,
- Da $2t = \deg(z^{2t}) = \deg(h_{j-1} y_j - y_{j+1} h_j) = \deg h_{j-1} + \deg y_j$ und $\deg h_{j-1} \geq t$, folgt $\deg \ell = \deg y_j = 2t - \deg h_{j-1} \leq t$.
- Analog folgt aus $2t - 1 \geq \deg s = \deg(h_{j-1} x_j - x_{j-1} h_j) = \deg h_{j-1} + \deg x_j$, dass $\deg u \leq 2t - 1 - t = t - 1$ und selbiges für w.

Gegeben: $\mathbf{d}$.

Gesucht: Fehler $\mathbf{e}$ beziehungsweise Mitteilung, dass ein Fehler von zu hohem Gewicht vorzuliegen scheint.

Algorithmus:

1. Führe den erweiterten Euklidischen Algorithmus für $f = z^{2t}$ und $g = s(z)$ durch und stoppe, falls $\deg h_j < t$ und $\deg h_{j-1} \geq t$.
2. Setze
$$\ell(z) := y_j(z)/y_j(0), \quad u(z) := x_j(z)/y_j(0), \quad w(z) := h_j(z)/y_j(0).$$
Falls $w = 0$, dann **Return** FEHLER.
Falls $\deg u \geq \deg \ell$ oder $\deg w \geq \deg \ell$, dann **Return** FEHLER.
3. Faktorisiere
$$\ell(z) = \prod_{j \in M} (1 - \beta^j z)$$
über $\mathbb{F}_q$ (oder **Return** FEHLER, wenn ℓ nicht in Linearfaktoren zerfällt). Lese von der Parzialbruchzerlegung von
$$\frac{w(z)}{\ell(z)} = \sum_{j \in M} e_j \beta^j \frac{1}{1 - \beta^j z}$$
die e_j ab.
4. **Return** $\mathbf{e}$.

Abbildung 4.1: Algorithmus

Sei nun $y_j(0) = 0$. Dann muss der Algorithmus FEHLER zurückgeben. Die Polynome h_j, x_j und y_j erfüllen alle gewünschten Eigenschaften, bis auf $\ell(0) = 1$. Im Beweis der Eindeutigkeit des Lemma 4.10 haben wir gezeigt, dass ℓ assoziiert zu y_j ist (gleich bis auf eine Konstante). Dazu haben wir $\ell(0) = 1$ noch nicht benutzt. Wir haben also, dass $\ell = f \cdot y_j$ für ein $f \in \mathbb{F}_q$. Wenn wir 0 einsetzen folgt
$$1 = \ell(0) = f \cdot y_j(0) = 0$$
ein Widerspruch. □

4.4 Reed-Solomon-Codes und Burst Error Correction

In manchen Anwendungen ist es sehr wahrscheinlich, dass Fehler gruppiert auftreten (z.B. Kratzer auf einer CD). Diese Fehler nennen sich "BurstErrors. Bei einem Binärcode müssen wir jedes derartig zerstörte Bit als Fehler ansehen; dadurch erreicht man meist relativ rasch die Minimaldistanz eines Codes. Daher wollen wir folgende Variante betrachten. Wir fassen k Bits zu einem Block zusammen und sehen das als Koordinatenvektor eines Elements des $\mathbb{F}_{2^k}$ an. Damit betreffen die Burst-Errors nur mehr relativ wenige Blöcke und ein passender Code über $\mathbb{F}_{2^k}$ kann das korrigieren.

Definition. Der Reed-Solomon-Code(k, t) ist der BCH-Code$(1, t)$ über $\mathbb{F}_{2^k}$; also mit Prüfmatrix
$$\begin{pmatrix} \beta^{q-2} & \dots & \beta & 1 \\ \beta^{2(q-2)} & \dots & \beta^2 & 1 \\ \vdots & & \vdots & \vdots \\ \beta^{2t(q-2)} & \dots & \beta^{2t} & 1 \end{pmatrix},$$

wobei $q = 2^k$ und β ein primitives Element von $\mathbb{F}_q$.

Satz 4.13 (Eigenschaften von Reed-Solomon-Codes)**.** *Wir betrachten den Reed-Solomon-Code(k, t).*

1. *Blocklänge:* $2^k - 1$,
2. *Generatorpolynom:* $(X - \beta)(X - \beta^2) \cdots (X - \beta^{2t})$,
3. *Dimension:* $2^k - 1 - 2t$,
4. *Minimaldistanz:* $2t + 1$,
5. *Burst-errors der Länge* $\leq k(t-1) + 1$ *können korrigiert werden.*

Beweis.

1. Die Blocklänge folgt durch Abzählen der Spalten.
2. Das Minimalpolynom von β^j über $\mathbb{F}_q$ ist $(X - \beta^j)$. Da das Generatorpolynom eines BCH-Codes, das kleinste gemeinsame Vielfache der Minimalpolynome ist, folgt alles.
3. Die Dimension ergibt sich als Differenz der Blocklänge und des Grades des Generatorpolynomes.
4. Die Minimaldistanz ist $\geq 2t + 1$, weil es sich um einen BCH-Code handelt. Andererseits ist die Minimaldistanz $\leq 2t + 1$, weil das Generatorpolynom ein Codewort ist und vom Grad $2t$, und damit ein Gewicht $\leq 2t + 1$.
5. $k(t-1) + 1$ hintereinanderliegende Bits können nur t k-Bit-Blöcke belegen, weil für die Belegung von $t + 1$ k-Bit-Blöcken braucht man mindestens $(t-1)k + 2$ aufeinanderfolgende Bits.

□

4.5 Schranken für Codes

In diesem Abschnitt wollen wir einige Schranken für die Parameter von Codes bestimmen. Einen ersten Vorgeschmack haben die Hamming-Codes im vorigen Kapitel geliefert. Deren asymptotische Rate war nämlich 1. An dieser Stelle wollen wir allgemeine Abschätzungen liefert. Zunächst benötigen wir ein Lemma für die Abschätzung der Elemente in einer Kugel

Lemma 4.14. *Sei $x \in \mathbb{F}_q^n$ und $r \geq 0$. Dann ist*

$$V(q, n, r) := |\overline{B(x, r)}| = \binom{n}{0} + \binom{n}{1}(q-1)^1 + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r.$$

Beweis. Für den Abstand k wählen wir k Positionen für Abweichungen ($\binom{n}{k}$ Möglichkeiten). An jeder dieser Position haben wir $(q-1)$ Möglichkeiten, also insgesamt $(q-1)^k$ Möglichkeiten. Dies ergibt zusammen

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

□

Als erste Schranke wollen wir die Anzahl der möglichen Codewörter bei gegebener Minimaldistanz abschätzen.

Satz 4.15 (Hamming-Schranke)**.** *Sei C ein Blockcode über $\mathbb{F}_q$ mit Blocklänge n ($C \subset \mathbb{F}_q^n$) und Minimaldistanz $2r + 1$. Dann gilt*

$$|C| \leq \frac{q^n}{V(q, n, r)}.$$

Beweis. Wegen der Minimaldistanz können r Fehler korrigiert werden. Jedem Codewort $\mathbf{c}$ wird damit eindeutig die Kugel $\overline{B(\mathbf{c}, r)}$ zugewiesen. Diese Kugeln müssen disjunkt sein und daher

$$\sum_{\mathbf{c} \in C} |\overline{B(\mathbf{c}, r)}| = |C| \cdot V(q, n, r) \leq q^n.$$

□

Beispiel. Sei C ein Hamming-Code. Dann ist $r = 1$, $n = 2^k - 1$ und $m = 2^k - 1 - k = n - k$. Die Hamming-Schranke ergibt also

$$|C| \leq \frac{2^n}{1 + (2^k - 1)} = 2^{n-k}.$$

Damit ist für Hamming-Codes diese Schranke scharf. Es gibt noch viele weitere Codes, wo die Hamming-Schranke scharf ist.

Als nächstes wollen wir einen Schranke für das Verhältnis Dimension zu Minimaldistanz geben.

Satz 4.16 (Singleton-Schranke)**.** *Sei $C \subset \mathbb{F}_q^n$ ein linearer Code mit $\dim C = m$ und Minimaldistanz d. Dann gilt:*

$$m \leq n - (d - 1).$$

Beweis. Wir definieren die Funktion

$$k : C \to \mathbb{F}_q^{n-d+1}$$
$$(c_1, \ldots, c_n) \mapsto (c_1, \ldots, c_{n-d+1})$$

(die „Kill"-Funktion). Wir zeigen zuerst, dass k injektiv ist. Angenommen es gilt $k(c_1, \ldots, c_n) = (c_1, \ldots, c_{n-d+1}) = (d_1, \ldots, d_{n-d+1}) = k(d_1, \ldots, d_n)$. Damit folgt aber, dass $\mathrm{d}((c_1, \ldots, c_n), (d_1, \ldots, d_n)) \leq d - 1$, und nachdem die Minimaldistanz d ist, gilt $(c_1, \ldots, c_n) = (d_1, \ldots, d_n)$.
Mit der Injektivität der Kill-Funktion folgt unmittelbar, dass

$$|C| \leq q^{n-d+1}.$$

□

Beispiel. Betrachte Reed-Solomon-Code über $\mathbb{F}_q$ mit $2t$ Zeilen, also Minimaldistanz $2t + 1$. Dann ist $n = q - 1$ und $m = n - 2t$ und die Singleton-Schranke ist scharf.

Die folgende Schranke liefert uns eine Konstruktion für einen Code bei gegebenen Blocklänge und Minimaldistanz.

Satz 4.17 (Gilbert-Varshamov-Schranke)**.** *Seien n und $d < n \in \mathbb{N}$. Dann gibt es einen Blockcode $C \subset \mathbb{F}_q^n$ mit Minimaldistanz $\geq d$ und*

$$|C| \geq \frac{q^n}{V(q, n, d - 1)}.$$

Weiters kann ein linearer Code mit dieser Eigenschaft gefunden werden.

Beweis. 1. Ohne Linearität: Für jedes Codewort $\mathbf{c} \in C$ gilt, dass $C \cap B(\mathbf{c}, d - 1) = \{\mathbf{c}\}$. Falls es ein $c_0 \in \mathbb{F}_q^n$ mit $c_0 \notin \bigcup_{c \in C} \overline{B(c, d - 1)}$, so könnte c_0 zu C hinzugefügt werden, ohne die Minimaldistanz unter d zu drücken. Wir können so lange Wörter hinzufügen, bis $\mathbb{F}_q^n \subset \bigcup_{c \in C} \overline{B(c, d - 1)}$. Also $q^n = |\mathbb{F}_q^n| \leq |C| \cdot V(q, n, d - 1)$. Daraus folgt

$$|C| \geq \frac{q^n}{V(q, n, d - 1)}.$$

2. Um dies für lineare Codes zu machen: Sei C linear (ohne die Schranke zu erfüllen), und es gebe ein $c_0 \notin \bigcup_{c\in C} \overline{B(c, d-1)}$. Dann setzen wir

$$C' := \operatorname{span}(C \cup \{c_0\}) = C + \operatorname{span}(c_0) = \left\{C - a \cdot c_0 \middle| c \in C, a \in \mathbb{F}_q^n\right\}.$$

Nun ist C' offensichtlich ein linearer Code, die Blocklänge bleibt unverändert und $C \subsetneq C'$. Es bleibt zu zeigen, dass die Minimaldistanz $\geq d$ ist. Für alle $c - ac_0$, mit $c \in C$ und $a \in \mathbb{F}_q^n \setminus \{0\}$ gilt:

$$\mathrm{d}(c - ac_0, 0) = \mathrm{d}(c, ac_0) = d(a^{-1}c, c_0) \geq d.$$

Damit ist alles gezeigt und wir können so weitermachen, wie im 1.Teil.

□

Beispiel. Zum Beispiel

- der $(7, 8)$-Paritätscheck-Code,
- der 3-fach Wiederholungs-Code,
- der abcxyz-Code,

erfüllen die Abschätzung.
BCH-Codes mit größeren Parametern schaffen es meistens nicht; dafür gibt es aber effizientere Fehlerprozessoren.

Schließlich wollen wir uns mit der Frage auseinandersetzen, was passiert wenn wir die Blocklänge n gegen unendlich gehen lassen. Dazu müssen wir zuerst $V(q, n, r)$ asymptotisch verstehen, und somit zuerst

$$\binom{n}{r}(q-1)^r.$$

In unseren Betrachtungen wollen wir das Verhältnis $\frac{r}{n} \approx \delta$ konstant bleiben lassen („relative Minimaldistanz“).

Lemma 4.18. *Sei q fest, $r(n) := \lfloor n\delta \rfloor$, $0 < \delta < \frac{q-1}{q}$. Dann gilt*

$$\lim_{n\to\infty} \frac{1}{n} \log_q \binom{n}{r(n)}(q-1)^{r(n)} = H_q(\delta),$$

wobei

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q(\delta) - (1-\delta)\log_q(1-\delta)$$

die Entropie ist.

Beweis. Für $n \to \infty$ gilt auch $r(n) \to \infty$ und $n - r(n) \to \infty$. Für $r(n)$ gilt asymptotisch

$$r(n) = n\delta + \mathcal{O}(1).$$

Mit der Stirling'schen Formel

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

erhalten wir

$$\log_q(n!) = \log_q(\sqrt{2\pi}) + \left(n + \frac{1}{2}\right)\log_q(n) - n\log_q(e) + \mathcal{O}(1).$$

Also

$$\begin{aligned}
&\frac{1}{n}\log_q \binom{n}{r}(q-1)^r \\
&= \frac{1}{n}\log_q(q-1) + 1\log_q(n) - \log_q(e) - \frac{r}{n}\log_q(r) + \frac{r}{n}\log_q(e) - \frac{n-r}{n}\log_q(n-r) + \frac{n-r}{n}\log_q(e) + \mathcal{O}(1) \\
&= \delta\log_q(q-1) + \log_q(n) - \delta\left(\log_q\left(\frac{r}{n}\right) + \log_q(n)\right) - (1-\delta)\left(\log_q\left(1-\frac{r}{n}\right) + \log_q(n)\right) + \mathcal{O}(1) \\
&= \delta\log_q(q-1) - \delta\log_q(\delta) - (1-\delta)\log_q(1-\delta) + \mathcal{O}(1).
\end{aligned}$$

□

Lemma 4.19. *$H_q(\delta)$ ist auf $\left[0, \frac{q-1}{q}\right]$ streng monoton wachsend und Markov. Es gilt*

$$H_q(\delta) \geq \delta \frac{q}{q-1}.$$

Beweis. Für die Ableitungen gilt

$$H_q'(\delta) > 0 \quad \text{und} \quad H_q''(\delta) < 0.$$

Außerdem ist $H_q(0) = 0$ und

$$H_q\left(\frac{q-1}{q}\right) = \frac{q-1}{q}\log_q(q-1) - \frac{q-1}{q}\log_q\left(\frac{q-1}{q}\right) - \frac{1}{q}\log_q\left(\frac{1}{q}\right) = -\log_q\left(\frac{1}{q}\right) = 1.$$

Damit liegt $H_q(\delta)$ über der Geraden durch $(0,0)$ und $\left(\frac{q-1}{q}, 1\right)$. □

Lemma 4.20. *Mit den Voraussetzungen von Lemma 4.18 gilt*

$$\lim_{n\to\infty} \frac{1}{n}\log_q V(q,n,r) = H_q(\delta).$$

Beweis. Sei $\delta < 1 - \frac{1}{q}$. Offensichtlich gilt

$$1 = (\delta + (1-\delta))^n = \sum_{k=0}^{n} \binom{n}{k} (q-1)^k (1-\delta)^{n-k} \left(\frac{\delta}{q-1}\right)^k.$$

Wir wollen nun zeigen, dass

$$(1-\delta)^{n-k}\left(\frac{\delta}{q-1}\right)^k \geq (1-\delta)^{n-\delta n}\left(\frac{\delta}{q-1}\right)^{\delta n}.$$

Kürzen auf beiden Seiten ergibt

$$\begin{aligned}
& (q-1)^{\delta n-k}(1-\delta)^{\delta n-k} \geq \delta^{\delta n-k} \\
\iff \quad & (q-1)(1-\delta) \geq \delta \\
\iff \quad & q-1 \geq \frac{\delta}{1-\delta} \\
\iff \quad & q-1 \geq -1 + \frac{1}{1-\delta} \\
\iff \quad & \frac{1}{q} \leq 1-\delta \\
\iff \quad & \delta \leq 1 - \frac{1}{q}
\end{aligned}$$

Oben einsetzen ergibt

$$\begin{aligned}
1 &\geq \left(\sum_{k=0}^{n} \binom{n}{k}(q-1)^k\right)\left(\frac{\delta}{q-1}\right)^{\delta n}(1-\delta)^{n(1-\delta)} \\
&\geq V(q,n,r) q^{n(\delta\log_q(\delta) - \delta\log_q(q-1) + (1-\delta)\log_q(1-\delta))} \\
&= V(q,n,r) q^{-nH_q(\delta)}.
\end{aligned}$$

Somit folgt mit Lemma 4.18, dass

$$H_q(\delta) \geq \frac{1}{n}\log_q V(q,n,r) \geq \frac{1}{n}\log_q \binom{n}{r}(q-1)^r = H_q(\delta) + o(1).$$

Damit gilt für den Limes

$$\lim_{n\to\infty} \frac{1}{n} \log_q V(q,n,r) = H_q(\delta).$$

□

Satz 4.21 (Asymptotische Gilbert-Varshamov-Schranke)**.** *Sei q eine Primzahlpotenz und $0 < \delta < \frac{q-1}{q}$ fest. Dann gibt es für jede natürliche Zahl n einen linearen Code $C_n \subset \mathbb{F}_q^n$, mit Minimaldistanz d_n, sodass $\lim_{n\to\infty} \frac{d_n}{n} \to \delta$, und*

$$\lim_{n\to\infty} \frac{\dim C_n}{n} = 1 - H_q(\delta) > 0.$$

Beweis. Wähle C_n so, dass

$$|C_n| \geq \frac{q^n}{V(q,n,r(n))}$$

mit $r(n) = \lfloor \delta n \rfloor$. Dieser hat nach der Gilbert-Varshamov-Schranke (Satz 4.17) Minimaldistanz $d_n = r(n) + 1$. Dann gilt

$$\lim_{n\to\infty} \frac{d_n}{n} = \delta.$$

Für die Dimension gilt

$$\dim C_n \geq \log_q \left(\frac{q^n}{V(q,n,r(n))} \right) = n - \log_q V(q,n,r(n))$$

und mit Lemma 4.19 und Lemma 4.20 folgt

$$\lim_{n\to\infty} \frac{\dim C_n}{n} \geq \lim_{n\to\infty} \left(1 - \frac{\log_q V(q,n,r(n))}{n} \right) = 1 - H_q(\delta) > 0.$$

□

Beispiel.

- Für Reed-Solomon-Codes gilt $q = 2^k$ und $n = 2^k - 1$. Wir wählen ein $\varepsilon > 0$ und $t = \lfloor \frac{n\varepsilon}{2} \rfloor$. Die relative Minimaldistanz ist

  $$\frac{2t+1}{n} \to \epsilon > 0.$$

  Für die Rate gilt

  $$\frac{2^k - 1 - 2t}{2^k - 1}.$$

- Für BCH-Codes gilt $n = q^k - 1$. Wir erhalten, dass die Minimaldistanz $\geq 2t + 1$ und die Dimension $\geq n - 2tk$ sind. Für die relative Minimaldistanz folgt asymptotisch

  $$\frac{2t+1}{n} \to \delta,$$

  wobei wir $t := \lfloor \frac{n\delta}{2} \rfloor$ setzen. Das ergibt für die Rate aber

  $$\frac{n - 2tk}{n} = 1 - 2\frac{tk}{n} = 1 - 2\frac{\delta}{2}k + \mathcal{O}(1) \to -\infty.$$

  Für eine bessere Asymptotik benötigt man eine untere Abschätzung für die Minimaldistanz und die Dimension. Selbst dann geht die Rate gegen 0, wenn die relative Minimaldistanz gegen $\delta > 0$ nach unten beschränkt bleibt.

4.6 Klassische Goppa-Codes

Bei den BCH-Codes hatten wir zur Decodierung folgende Relation:

$$s(z) \equiv \frac{w(z)}{\ell(z)} \pmod{z^{2t}}.$$

Die Idee der klassischen Goppa-Codes ist es nun, ein anders Polynom als z^{2t} zu verwenden.

Definition. Sei $\mathbb{F}_q$ ein endlicher Körper, $\mathbb{F}_{q^k}$ eine Körpererweiterung von $\mathbb{F}_q$. Dann wähle eine Teilmenge $P \subset \mathbb{F}_{q^k}$ und ein Polynom $g \in \mathbb{F}_{q^k}[Z]$, sodass $\forall \beta \in P : g(\beta) \neq 0$. Dann definiere wir den klassischen Goppa-Code $\mathrm{GC}(P, g)$ als

$$\mathrm{GC}(P,g) := \left\{ \mathbf{c} \in \mathbb{F}_q^{|P|} \middle| \sum_{\beta \in P} \frac{c_\beta}{Z-\beta} \equiv 0 \pmod{g} \right\}$$

Bemerkung.

1. Da $g(\beta) \neq 0$, folgt $\mathrm{ggT}(Z-\beta, g) = 1$ und damit ist $\frac{1}{Z-\beta} \pmod{g}$ überhaupt sinnvoll.
2. Jeder BCH-Code ist auch ein Goppa-Code mit

$$g = Z^{2t}, \quad P = \mathbb{F}_q^k \setminus \{\mathbf{0}\}.$$

Satz 4.22. *Ein Goppa-Code ist ein linearer Code der Blocklänge $|P|$, mit Minimaldistanz $\geq (g(z)) + 1$ und Dimension $\geq |P| - (\deg g) \cdot k$.*

Beweis. Da $\mathrm{ggT}(Z-\beta), g(Z)) = 1$ für $\beta \in P$, gibt es ein Polynom $h_\beta \in \mathbb{F}_{q^k}[Z]$ mit $(Z-\beta)h_\beta \equiv 1 \pmod{g}$. Das heißt,

$$\mathbf{c} \in \mathrm{GC}(P,g) \iff \sum_{\beta \in P} c_\beta h_\beta \equiv 0 \pmod{g}.$$

Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $\deg h_\beta < \deg g$ ist. Dann ist auch $\deg \sum_{\beta \in P} c_\beta h_\beta < \deg g$ und somit folgt

$$\sum_{\beta \in P} c_\beta h_\beta = 0.$$

Wir machen Koeffizientenvergleich in Z und verwenden einen Erzeuger α von $\mathbb{F}_{q^k}$ über $\mathbb{F}_q$ um ein lineares Gleichungssystem für c_β mit $(\deg g) \cdot k$ Zeilen zu bekommen.
Für die Minimaldistanz sei $\mathbf{0} \neq \mathbf{c} \in \mathrm{GC}(P,g)$ und $P(\mathbf{c}) := \{\beta \in P : c_\beta \neq 0\}$. Dann gilt

$$\sum_{\beta \in P(\mathbf{c})} \frac{c_\beta}{Z-\beta} \equiv \sum_{\beta \in P(\mathbf{c})} \frac{c_\beta \prod_{\gamma \in P(\mathbf{c}) \setminus \{\beta\}} (Z-\gamma)}{\prod_{\gamma \in P(\mathbf{c})} (Z-\gamma)} \equiv 0 \pmod{g}.$$

Daraus folgt, dass

$$g \left| \sum_{\beta \in P(\mathbf{c})} c_\beta \prod_{\gamma \in P(\mathbf{c}) \setminus \{\beta\}} (Z-\gamma) \right.$$

und

$$\deg(g) \leq \deg \left(\sum_{\beta \in P(\mathbf{c})} c_\beta \prod_{\gamma \in P(\mathbf{c}) \setminus \{\beta\}} (Z-\gamma) \right) \leq |P(\mathbf{c})| - 1 = \mathrm{wt}(\mathbf{c}) - 1.$$

□

Die Fehlerkorrektur passiert auf die selbe Art und Weise wie im Fall von BCH-Codes.

Satz 4.23. *Klassische Goppa-Codes bilden eine asymptotisch gute Familie von Codes; d.h. es gibt eine Folge von Codes C_n mit relativer Minimaldistanz $\to \delta > 0$ und Rate $\to \varepsilon > 0$.*

Bemerkung. Das gilt leider nur für die relative Minimaldistanz und nicht für die designte Minimaldistanz; nur kann der Fehlerprozessor mit dieser Minimaldistanz nicht umgehen.

Beweisskizze. Wähle d und t so, dass $d \cdot V(q, q^k, d-1) < t \cdot N_{q^k}(t)$ ist (wobei $N_{q^k}(t)$ die Anzahl der irreduziblen Polynome vom Grad t in $\mathbb{F}_{q^k}$ ist. Für jedes Tupel $\mathbf{c}$ aus der geschlossenen Kugel $\overline{B(0, d-1)}$ soll das Polynom $c_\beta \prod_{\gamma \in P(\mathbf{c}) \setminus \{\beta\}} (Z - \gamma)$ nicht aus dem Code sein. Diese Polynome sind vom Grad $d-2$ und haben $\leq \frac{d-2}{t}$ irreduzible Faktoren vom Grad t. Damit folgt, dass für $\overline{B(0, d-1)}$ höchstens $V(q, q^k, d-1) \cdot \frac{d-2}{t}$ irreduzible Polynome vom Grad t verbraucht. Die Abschätzung $< t \cdot N_{q^k} t$ sagt uns, dass ein irreduzibles Polynom vom Grad t übrig bleibt. Dieses ist dann das gesuchte Polynom g. Diese Konstruktion können wir asymptotisch weiterführen. □

Anhang

A1 Etwas lineare Algebra

In diesem Anhang ist V ein endlichdimensionaler Vektorraum über einem Körper K, $F : V \to V$ eine lineare Abbildung.

Definition. Das Minimalpolynom von F ist das Polynom g kleinsten Grades, das normiert ist und $g(F) = 0$ erfüllt.

Bemerkung. Laut Satz von Cayley-Hamilton gibt es jedenfalls ein Polynom mit diesen Eigenschaften, nämlich das charakteristische Polynom oder das negative charakteristische Polynom von F.

Proposition A1.1. *Mit den Bezeichnungen der Definition gilt:*

$$\forall h \in K[X] : h(F) = 0 \Rightarrow g \mid h.$$

Insbesondere ist g dadurch eindeutig definiert.

Beweis. Sei $\mathrm{Ann}(F)$ der Annihilator von F, d.h.

$$\mathrm{Ann}(F) := \{h \in K[X] \mid h(F) = 0\}.$$

Das ist ein Ideal von $K[X]$, denn:

- $h_1(F) = 0 \wedge h_2(F) = 0 \Rightarrow (h_1 - h_2)(F) = h_1(F) - h_2(F) = 0 - 0 = 0.$
- Für $h \in \mathrm{Ann}(F)$ und $g \in K[X]$ gilt: $hg(F) = h(F)g(F) = 0g(F) = 0.$

Nachdem K ein Körper ist, ist $K[X]$ ein Hauptidealbereich. Also gibt es ein $g \in K[X]$ mit $\mathrm{Ann}(F) = (g) = \{fg \mid f \in K[x]\}$. Ohne Beschränkung der Allgemeinheit wählen wir g normiert und haben das Minimalpolynom gefunden. □

Korollar A1.2. *Das Minimalpolynom teilt das charakteristische Polynom. Falls das Minimalpolynom vom Grad* $\dim_K V$ *ist, so gilt:*

$$\textit{Minimalpolynom} = \pm \textit{charakteristisches Polynom}.$$

Beweis. Das charakteristische Polynom ist wegen des Satzes von Cayley-Hamilton ein Annihilator von F. Wenn beide Polynome selben Grad haben, so unterscheiden sie sich nur um eine multiplikative Konstante. Das Minimalpolynom ist laut Definition normiert, das charakteristische Polynom hat den Leitkoeffizienten ± 1, also ist die Konstante ± 1. □

Lemma A1.3. *Sei $r \in \mathbb{N}$, $\lambda \in K$ und J_r ein Jordanblock der Länge r zum Eigenwert λ, d.h.*

$$J_r = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix}$$

Dann ist das Minimalpolynom von J_r gleich $(X-\lambda)^r$.

Beweis. $(X-\lambda)^r \in \mathrm{Ann}(J_r)$. Gibt es ein Polynom vom Grad $< r$, das J_r annihiliert, so sind $J_r^{r-1}v, \ldots, J_r v, v$ für jeden Vektor v linear abhängig.
Für den r-ten Einheitsvektor ist das ein Widerspruch. (Nachrechnen!) □

Bemerkung. Auf diese Weise lässt sich das Minimalpolynom einer linearen Abbildung verstehen, sofern das charakteristische Polynom über K in Linearfaktoren zerfällt.

Satz A1.4. *Sei K ein Körper, V ein n-dimensionaler K-Vektorraum, $F : V \to V$ linear. Dann sind folgende Aussagen äquivalent:*

1. *Das Minimalpolynom von F ist gleich dem charakteristischen Polynom von F (bis auf ein Vorzeichen).*
2. *Es gibt einen Vektor $v \in V$, sodass $v, F(v), \ldots, F^{n-1}(v)$ eine Basis von V ist.*

Beweis.

$\neg 1 \Rightarrow \neg 2$: Wir wissen: Minimalpolynom teilt charakteristisches Polynom. Wenn nicht gleich, so ist der Grad des Minimalpolynoms kleiner als der Grad des charakteristischen Polynoms.

$$\text{Minimalpolynom} = \sum_{j=0}^{n-1} a_j X^j$$

Damit folgt, dass

$$\sum_{j=0}^{n-1} a_j F^j(v) = \left(\sum_{j=0}^{n-1} a_j F^j\right)(v) = 0.$$

Also ist $v, F(v), \ldots, F^{n-1}(v)$ linear abhängig und somit keine Basis.

$1 \Rightarrow 2$: Sei f das Minimalpolynom von F, $f = f_1^{r_1} \cdots f_m^{r_m}$ die Zerlegung in irreduzible Polynome. Das ist möglich, weil $K[X]$ ein faktorieller Ring (ZPE-Ring) ist. Für $v \in V$ setzen wir

$$\mathrm{Ann}(F, v) := \{g \in K[X] \mid g(F)(v) = 0\}.$$

1. Behauptung: $\forall v \in V : \mathrm{Ann}(F, v) \trianglelefteq K[X]$.

   Beweis.
   - $0 \in \mathrm{Ann}(F, v)$.
   - $\forall g_1, g_2 \in \mathrm{Ann}(F, v) : (g_1 - g_2)(F)(v) = g_1(F)(v) - g_2(F)(v) = 0 - 0 = 0$.
   - $\forall H \in K[X], g \in \mathrm{Ann}(F, v) : (hg)(F)(V) = h(F)(v)g(F)(v) = h(F)(v)0 = 0$.

   also ist $\mathrm{Ann}(F, v)$ ein Ideal (sogar ein Hauptideal). □

2. Behauptung: für $j \in \{1, \ldots m\}$ gibt es ein v_j mit $\mathrm{Ann}(F, v_j) = (f_j^{r_j})$.

   Beweis. Es gilt, dass $\frac{f}{f_j}$ ein Polynom ist, aber kein Annihilator von F. Das heißt: $\frac{f}{f_j}(F) \neq 0$. Es gibt daher ein $w_j \in V$ mit $\frac{f}{f_j}(F)(w_j) \neq 0$.
   Setze $v_j := \frac{f}{f_j^{r_j}}(F)(w_j)$. Es gilt: $f_j^{r_j}(v_j) = f(F)(w_j) = 0$, also ist $f_j^{r_j} \in \mathrm{Ann}(F, v_j)$. Allerdings: $f_j^{r_j-1}(v_j) = \frac{f}{f_j}(F)(w_j) \neq 0$ laut Konstruktion von w_j. Also $f_j^{r_j-1} \notin \mathrm{Ann}(F, v_j)$. Es folgt:

   $$\mathrm{Ann}(F, v_j) = (g) \text{ für ein } g \text{ mit } g \mid f_j^{r_j} \text{ und } g \nmid f_j^{r_j-1}.$$

   Nachdem $K[X]$ ein faktorieller Ring (ZPE-Ring) ist, folgt aus der Eindeutigkeit der Primfaktorzerlegung, dass $g = f_j^{r_j}$. □

3. Behauptung: Seien $v, w \in V$ mit $\mathrm{Ann}(F, v) = (g)$ und $\mathrm{Ann}(F, w) = (h)$ für teilerfremde Polynome g und h. Dann ist $\mathrm{Ann}(F, v + w) = (gh)$.

   Beweis.

$$\begin{aligned}(gh)(F)(v+w) &= (gh)(F)(v) + (gh)(F)(w)\\ &= (hg)(F)(v) + (gh)(F)(w)\\ &= (h(F) \circ g(F))(v) + (g(F) \circ h(F))(w)\\ &= h(F)(g(F)(v)) + g(F)(h(F)(w))\\ &= 0,\end{aligned}$$

   also ist $gh \in \mathrm{Ann}(F, v + w) = (g_1 h_1)$, wobei $g_1 \mid g$ und $h_1 \mid h$.
   Schreibe $g = g_1 g_2$ und $h = h_1 h_2$ für passende Polynome.

$$\begin{aligned}(gh_1)(F)(v+w) &= (g_2 g_1 h_1)(F)(v+w)\\ &= g_2(F)((g_1 h_1)(F)(v+w))\\ &= 0.\end{aligned}$$

   Andererseits:

$$\begin{aligned}(gh_1)(F)(v+w) &= (h_1 g)(F)(v) + (gh_1)(F)(w)\\ &= 0 + (gh_1)(F)(w),\end{aligned}$$

   daher gilt $gh_1 \in \mathrm{Ann}(F, w) = (h_1 h_2)$. Es gilt $h_1 h_2 \mid gh_1$, also $h_2 \mid g$. Laut Konstruktion von h_2 gilt $h_2 \mid h$. Somit teilt h_2 den größten gemeinsamen Teiler und ist daher konstant. Analoges gilt für g_2. □

Insgesamt gibt es ein $v \in V$ mit $\mathrm{Ann}(F, v) = (f)$, somit sind $v, F(v), \ldots, F^{n-1}(v)$ linear unabhängig. □

Bemerkung. Der Fall in Satz A1.4 entspricht genau dem Fall, wo es pro Eigenwert genau einen Jordanblock gibt, das heißt jeder Eigenwert hat geometrische Vielfachheit 1.