

Endliche Körper und Codierung

Florian Lehner, Jan Pöschko

21. Mai 2007

Inhaltsverzeichnis

1	Endliche Körper	3
1.1	Wohlbekanntes	3
1.2	Zwischenkörperstruktur	3
1.3	Automorphismenstruktur	5
1.4	Basen und andere Darstellungen von Körperelementen	6
2	Polynome über endlichen Körpern	9
2.1	Kreisteilungspolynome und Einheitswurzeln	9
2.2	Die Ordnung von Polynomen	12
2.3	Irreduzible Polynome	14
2.4	Faktorisierung von Polynomen (Berlekamp-Algorithmus)	16
3	Grundbegriffe der Codierungstheorie	19
3.1	Einführung	19
3.2	Blockcodes, Distanz, Hamminggewicht	21
3.3	Lineare Codes	23
	Anhang	27
A1	Etwas lineare Algebra	27

Bemerkung. p bezeichnet in diesem Skriptum (außer anders angemerkt) immer eine Primzahl.

Bemerkung. Dieses Skriptum enthält vermutlich noch einige Fehler. Sollte also jemand einen Fehler oder eine Ungereimtheit entdecken, schreibt mir (lehner@student.tugraz.at) bitte ein E-Mail. Danke.

Kapitel 1

Endliche Körper

1.1 Wohlbekanntes

Ein endlicher Körper ist 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} .
- $\mathbb{F}_p = \mathbb{Z}_p$ mit Addition und Multiplikation modulo p .

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 . $f = X^2 + 1$ hat keine Nullstelle in \mathbb{F}_3 , ist also irreduzibel, da es ein Polynom vom Grad 2 ist. Also ist

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

Wie können wir in diesem Körper 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 $\text{ggT}(f, g) = 1$ ist. Die Lösung liefert der erweiterte euklidische Algorithmus.

Wir wissen weiters:

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

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 1.1. 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 eindeutigen Primfaktorzerlegung in \mathbb{Z} muss $|K| = p^k$ für ein passendes k sein. Es gilt $p^n = p^{kr}$, also $n = kr$ beziehungsweise $k \mid n$. \square

Satz 1.1 (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

$$(\alpha + \beta)^r = \alpha^r + \beta^r = \alpha + \beta \quad (\text{laut Algebra-Übung})$$

$$(\alpha\beta)^r = \alpha^r \beta^r = \alpha\beta$$

$$(-1)^r = -1 \quad (\text{für ungerades } r \text{ klar, bei gerader Charakteristik gibt es keine Vorzeichenfehler})$$

$$\left(\frac{1}{\alpha}\right)^r = \frac{1}{\alpha^r} = \frac{1}{\alpha} \quad (\text{für } \alpha \neq 0)$$

- $|M| = r$:

- $|M| \leq r$:

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

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

Weiters gilt nun

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

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. \square

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

Lemma 1.2. Sei f ein irreduzibles Polynom in $\mathbb{F}_q[X]$ vom Grad m und $n \in \mathbb{N}$. Dann gilt

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

Beweis. „ \Leftarrow “ Wir wissen aufgrund der Rechnung im Beweis von Satz 1.1, dass $X^{q^m} - X \mid X^{q^n} - X$. Es genügt also, $f \mid X^{q^m} - X$ zu zeigen.

Der Zerfällungskörper von $X^{q^m} - X$ ist \mathbb{F}_{q^m} . Wir wissen, dass \mathbb{F}_q ein Teilkörper von \mathbb{F}_{q^m} und $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$ ist.

Nun erweitern wir \mathbb{F}_{q^m} um eine Nullstelle α von f . Da $f(\alpha) = 0$ und $f \in \mathbb{F}_q[X]$, sowie $\deg f = m$ ist, gilt

$$m \geq [\mathbb{F}_{q^m}(\alpha) : \mathbb{F}_q] = [\mathbb{F}_{q^m}(\alpha) : \mathbb{F}_{q^m}] [\mathbb{F}_{q^m} : \mathbb{F}_q].$$

Somit muss $\mathbb{F}_{q^m}(\alpha) = \mathbb{F}_{q^m}$ sein, also ist $\alpha \in \mathbb{F}_{q^m}$ und folglich eine Nullstelle von $X^{q^m} - X$. Da f das Minimalpolynom von α über \mathbb{F}_q ist, gilt $f \mid X^{q^m} - X$.

„ \Rightarrow “ \mathbb{F}_{q^n} ist der Zerfällungskörper von $X^{q^n} - X$. Da f dieses Polynom teilt, ist f das Produkt von Linearfaktoren in $\mathbb{F}_{q^n}[X]$. Es gibt also eine Nullstelle $\alpha \in \mathbb{F}_{q^n}$ von f . Somit ist $\mathbb{F}_q(\alpha)$ ein Teilkörper von \mathbb{F}_{q^n} .

Weil f das Minimalpolynom von α ist, gilt $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. $\mathbb{F}_q(\alpha)$ hat somit q^m Elemente.

Laut Teilkörperstruktur gilt $m \mid n$. □

Lemma 1.3. 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:

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

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, also $\alpha^{q^j} = \alpha^{q^k}$ für gewisse $0 \leq j < k \leq m-1$. 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 $X^{q^l} - X$. f teilt also $X^{q^l} - X$ und laut Lemma 1.2 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. 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.

Φ_q erfüllt analoge Eigenschaften.

Definition (Automorphismengruppe).

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

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

Satz 1.2 (Automorphismenstruktur). *Sei q eine Primzahlpotenz, $m \in \mathbb{N}$. Dann ist $\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m})$ eine zyklische Gruppe der Ordnung m , die von $\Phi_q : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$, $x \mapsto x^q$ erzeugt wird, also:*

$$\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = \{ \text{id}, \Phi_q, \Phi_q^2, \dots, \Phi_q^{m-1} \}.$$

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 $\varphi \in \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m})$. Dann gilt

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

$\varphi(\alpha)$ ist also eine Nullstelle von f . Laut Lemma 1.3 gibt es somit ein $j \in \{0, \dots, m-1\}$ mit $\varphi(\alpha) = \alpha^{q^j} = \Phi_q^j(\alpha)$.

Sei nun $\beta \in \mathbb{F}_{q^m}$ beliebig. $\beta = \sum_{k=0}^{m-1} c_k \alpha^k$ für passende $c_k \in \mathbb{F}_q$. Es gilt:

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

das bedeutet, $\varphi = \Phi_q^j$.

Da die $\Phi_q^j(\alpha) = \alpha^{q^j}$ laut Lemma 1.3 paarweise verschieden sind, müssen die Φ_q^j paarweise verschieden sein. Also ist die Ordnung der Automorphismengruppe m . \square

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

1.4 Basen und andere Darstellungen von Körperelementen

Polynombasen

Für ein irreduzibles Polynom vom Grad m mit einer Nullstelle α ist $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ 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 $j \in \{m, \dots, 2m-2\}$, sowie viele Multiplikationen und Additionen im Grundkörper.
- Berechnung von Φ_q erfordert ebenfalls Reduktionen.

Logarithmische Darstellung

Die Einheitengruppe von \mathbb{F}_{q^m} ist zyklisch, das heißt es gibt ein $\alpha \in \mathbb{F}_{q^m}$, sodass

$$\mathcal{E}(\mathbb{F}_{q^m}) = \{\alpha^j \mid 0 \leq j \leq q^m - 1\}.$$

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

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

Normale Basen

Sei $\alpha \in \mathbb{F}_{q^n}$. Betrachte $\{\alpha, \Phi_q(\alpha), \Phi_q^2(\alpha), \dots, \Phi_q^{m-1}(\alpha)\}$. 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^n} ?

Satz 1.3 (Existenz normaler Basen). *Sei q eine Primzahlpotenz, $m \in \mathbb{N}$. Dann gibt es ein $\alpha \in \mathbb{F}_{q^m}$, sodass $\{\alpha, \Phi_q(\alpha), \Phi_q^2(\alpha), \dots, \Phi_q^{m-1}(\alpha)\}$ 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 1.4 (Artin). *Sei (G, \cdot) eine abelsche Gruppe, K ein Körper und $\varphi_1, \dots, \varphi_m$ paarweise verschiedene Homomorphismen von $G \rightarrow \mathcal{E}(K)$. Dann gibt es für jedes Tupel $(a_1, \dots, a_m) \in K^m \setminus \{0, \dots, 0\}$ ein $g \in G$ mit*

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

Beweis. Induktion nach m :

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

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

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

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

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

$$a_1\varphi_1(h)\varphi_1(g) + \dots + a_m\varphi_m(h)\varphi_m(g).$$

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

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

gilt für alle g . Widerspruch zur Induktionsannahme. □

Beweis von Satz 1.3. $\Phi_q : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ ist \mathbb{F}_q -Automorphismus, also auch eine \mathbb{F}_q -lineare Abbildung. Weiters sind $\text{id}, \Phi_q, \dots, \Phi_q^{m-1}$ paarweise verschiedene (Satz 1.2) Homomorphismen $\mathcal{E}(\mathbb{F}_{q^m}) \rightarrow \mathcal{E}(\mathbb{F}_q)$. Also gibt es laut Lemma von Artin kein Tupel $(a_1, \dots, a_m) \in K^m \setminus \{0, \dots, 0\}$, sodass $***$. Das Minimalpolynom von Φ_q hat also $\text{Grad} \geq m$. Das charakteristische Polynom von Φ_q hat $\text{Grad} \leq m$. Somit gilt: Minimalpolynom = ± 1 charakteristisches Polynom = $X^m - 1$ weil $\Phi_q^m = \text{id}_{\mathbb{F}_{q^m}}$.

Laut Satz A1.1 gibt es also ein $\alpha \in \mathbb{F}_{q^m}$, sodass $\alpha, \Phi_q(\alpha), \dots, \Phi_q^{m-1}(\alpha)$ eine Basis von \mathbb{F}_{q^m} bilden. \square

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 $e_1 = (1, 0, \dots, 0)^t$. Es gilt $Ae_1 = e_2, A^2e_1 = e_3, \dots, A^{m-1}e_1 = e_m$. Also ist $\{A^j e_1 \mid 0 \leq j \leq m-1\}$ eine Basis von \mathbb{F}_q^m und laut Satz A1.1 Minimalpolynom = $(-1)^m$ charakteristisches Polynom = $(-1)^m \det(A - XI)$. Durch Entwicklung nach der ersten Spalte erhalten wir für diese Determinante 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. Sehe $\mathbb{F}_{q^m} \simeq \text{span}\{I, A, A^2, \dots, A^{m-1}\}$. A verhält sich gleich wie eine abstrakte Nullstelle α von f .

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 $p \nmid n$.

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

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

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 $E^{(n)} = E^{(m)}$. \square

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 2.1. 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 $\beta \in P^{(k)}$. \square

Proposition 2.2. 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 $|\zeta^a| = n \Leftrightarrow a := \text{ggT}(\alpha, n) = 1$, weil $\zeta^{al} = 1 \Leftrightarrow n \mid al \Leftrightarrow n \mid l$. Somit ist

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

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 $X^k - 1$ in $K^{(n)}$ Linearfaktoren, somit $K^{(k)} \subseteq K^{(n)}$ und ich kann auf obigen Fall verweisen. \square

Korollar 2.1. $n = \sum_{k|n} \varphi(k)$.

Beweis. Kombiniere die letzten beiden Propositionen. \square

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

Definition. Sei $n \in \mathbb{N}$, K ein Körper der Charakteristik $p \geq 0$, $p \nmid n$. Definiere 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 2.3. *Bezeichnungen wie in der Definition, dann gilt in $K^{(n)}$:*

$$G - k(X) = \prod_{\beta \in P^{(k)}} (X - \beta)$$

und $G_k(X) \in K[X]$.

Beweis. Induktion nach k :

$k = 1$ Trivial.

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

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

Wir kürzen und erhalten:

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

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

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

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

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

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

Wie sieht die Primfaktorzerlegung von Kreisteilungspolynomen aus?

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

Satz 2.2 (Primfaktorzerlegung von Kreisteilungspolynomen über endlichen Körpern). *Sei q eine Primzahlpotenz, $n \in \mathbb{N}$ mit $\text{ggT}(q, n) = 1$. Weiters sei d die Ordnung von $(q + n\mathbb{Z})$ in $\mathcal{E}(\mathbb{Z}/n\mathbb{Z})$, also $d = \min\{k \in \mathbb{N} \mid q^k \equiv 1 \pmod{n}\}$. 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 f ein irreduzibler Teiler von G_n in $\mathbb{F}_q[X]$ vom Grad m . Sei $k \in \mathbb{N}$. Behauptung: f zerfällt in \mathbb{F}_{q^k} genau dann in Linearfaktoren, wenn $q^k \equiv 1 \pmod{n}$ ist.

- f zerfällt über \mathbb{F}_{q^k} in Linearfaktoren
- $\Leftrightarrow f$ hat Nullstelle $\beta \in \mathbb{F}_{q^k}$ (Satz 1.2)
- $\Leftrightarrow f$ 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 $n \mid q^k - 1$
- $\Leftrightarrow q^k \equiv 1 \pmod{n}$.

$d = \min\{k \in \mathbb{N} \mid q^k \equiv 1 \pmod{n}\} = \min\{k \in \mathbb{N} \mid f \text{ zerfällt über } \mathbb{F}_{q^k} \text{ in Linearfaktoren.}\} = m$.

Also hat jeder irreduzible Faktor von G_n hat 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. \square

Korollar 2.2. Sei q eine Primzahlpotenz, $n \in \mathbb{N}$ mit $\text{ggT}(n, q) = 1$. \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 2.1. 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 $X^l + (f) \in \mathbb{F}_q[X]/(f)$, $0 \leq l \leq q^m - 1$. Die Folge hat q^m Elemente.

$X^l + (f) \neq 0$ für alle l , weil sonst $X^l = g(X)f(X)$ in $\mathbb{F}_q[X]/(f)$. Einsetzen von 0 ergäbe $0 = g(0)f(0)$, somit $X \mid g(X)$, also $X^{l-1} + f = 0$, aber $X^0 + (f) = 1 + (f) \neq 0$.

Somit habe ich q^m Elemente in $\mathbb{F}_q[X]/(f)$ mit $q^m - 1$ Elementen. Laut Schubfachschluss gilt $X^r \equiv X^s \pmod{(f)}$ 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 $\text{ggT}(X, f) = 1$ und folglich $f \mid X^{s-r} - 1$. \square

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

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

Proposition 2.4. Sei $f \in \mathbb{F}_q[X]$ irreduzibel mit $\deg f = m$, $f(0) \neq 0$ (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 $\mathcal{E}(\mathbb{F}_{q^m})$.

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 $\mathcal{E}(\mathbb{F}_{q^m})$ das minimale l mit $\alpha^l = 1$. \square

Korollar 2.3. Sei $f \in \mathbb{F}_q[X]$ und α eine Nullstelle von f in \mathbb{F}_{q^m} dann ist α genau dann ein primitives Element, wenn die Ordnung $\text{ord}(f) = q^m - 1$ ist.

Beweis. α ist primitives Element $\Leftrightarrow |\alpha| = |\mathcal{E}(\mathbb{F}_{q^m})| = q^m - 1$. \square

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

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

Lemma 2.2. 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:

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

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: $X^n - 1 = X^{mt} - 1 = (X^m - 1)(X^{(m-1)t} + X^{(m-2)t} + \dots + 1)$. \square

Korollar 2.5. $\text{ggT}(X^m - 1, X^n - 1) = X^{\text{ggT}(m, n)} - 1$.

Beweis. Wir wissen: $(X^k - 1) \mid \text{ggT}(X^m - 1, X^n - 1) \Leftrightarrow k \mid \text{ggT}(m, n)$. Es bleibt also nur noch zu zeigen, dass des ggT die Form $X^k - 1$ hat.

Ohne Beschränkung der Allgemeinheit sei $n > m$. Induktion über m :

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

$m - 1 \rightarrow m$: Für $n = mt + r$ gilt

$$\text{ggT}(X^m - 1, X^n - 1) = \text{ggT}(X^m - 1, X^{n-tm} - 1) \quad (\text{Euklidischer Algorithmus})$$

und wir können die Induktionsvoraussetzung anwenden. \square

Proposition 2.5. Seien $f, g \in \mathbb{F}_q[X]$ mit $\text{ggT}(f, g) = 1$, $f \neq 0$ und $g \neq 0$, dann gilt:

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

Beweis. Sei $h = fg$. Wenn h das Polynom $X^e - 1$ teilt, dann auch f und g , also $f \mid \text{ggT}(X^e - 1, X^{\text{ord } f} - 1)$ beziehungsweise $g \mid \text{ggT}(X^e - 1, X^{\text{ord } g} - 1)$. Der ggT ist aber bekannt, also gilt $f \mid X^{\text{ggT}(e, \text{ord } f)} - 1$. Es muss also $\text{ggT}(e, \text{ord } f) = \text{ord } f$ sein. Analog dazu ist $\text{ggT}(e, \text{ord } g) = \text{ord } g$.

Somit sind sowohl $\text{ord } f$ als auch $\text{ord } g$ Teiler von e , also auch das kgV der beiden. $\text{ord } h$ ist das minimale e für das das alles gelten muss, also $\text{ord } h = \text{kgV}(\text{ord } f, \text{ord } g)$. \square

Proposition 2.6. 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:

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

Beweis. Definiere $g := f^b$, $k := \text{ord } f$ und $l = \text{ord } g$. 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 $j = t$. \square

Satz 2.3 (Ordnung von Polynomen). Sei $f \in \mathbb{F}_q[X]$, $f = f_1^{b_1} \dots f_r^{b_r}$ mit paarweise verschiedenen irreduziblen $f_j \in \mathbb{F}_q[X]$. Sei weiters $t \in \mathbb{N}$ minimal mit $p^t \geq \max b_j$, wobei $p = \chi(\mathbb{F}_q)$. Dann gilt

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

Beweis. Es gilt

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

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

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

Proposition 2.7. *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 vom Grad n der Ordnung e , wobei $d = m$ die Ordnung von q mod e ist.*

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

2.3 Irreduzible Polynome

Satz 2.4. *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*

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

wobei μ die Möbiussche μ -Funktion ist, also

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

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

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

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 $(X^{q^n} - X)' = q^n X^{q^n-1} - 1 = -1$.

Da P und $X^{q^n} - X$ beide normiert sind, folgt

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

Sortiere P nach Graden:

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

Berechne den Grad doppelt (inneres Produkt hat $N_q(d)$ Faktoren):

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

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

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

Dividiere durch n . □

Beispiel.

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

Korollar 2.6. 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)

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

Lemma 2.3. *Wenn man das Faktorisierungsproblem für quadratischfreie 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:

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

für passende b_i (siehe Übung).

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

2. $f' \neq 0$ und $d = \text{ggT}(f, f')$ ist nicht konstant. dann ist d ein Polynom mit $\text{Grad } 1 < \text{deg } d \leq \text{deg } f' \leq \text{deg } f$ und $d \mid f$. Schreibe $f = d \frac{f}{d}$ und bastle die Faktorisierung von f aus den Faktorisierungen von d und $\frac{f}{d}$, die beide kleineren Grad haben, zusammen.
3. $f' \neq 0$ und $\text{ggT}(f, f') = \text{const}$. Dann ist f quadratischfrei und wir müssen wirklich arbeiten. \square

Proposition 2.8. *Sei $f \in \mathbb{F}_q[X]$ quadratischfrei mit $f = P_1 \cdots P_r$ für irreduzible Polynome p_j . Dann ist*

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

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:

- $\text{deg } Q \leq \max(\text{deg } Q_1, \text{deg } Q_2) < \text{deg } f$
- $Q^q = (\alpha Q_1 + \beta Q_2)^q = \alpha^q Q_1^q + \beta^q Q_2^q \equiv \alpha Q_1 + \beta Q_2 \pmod{f}$.

2. 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 $j \in \{1, \dots, r\}$. Offensichtlich gilt $P_j \mid \prod_{\alpha \in \mathbb{F}_q} (Q(X) - \alpha)$. Also gibt es ein $\alpha_j \in \mathbb{F}_q$ mit $P_j \mid Q(X) - \alpha_j$, und damit $Q(X) \equiv \alpha_j \pmod{P_j}$.

α_j ist aufgrund der Eindeutigkeit der Division mit Rest eindeutig bestimmt.

Betrachte ab jetzt die Abbildung $\Phi : V_f \rightarrow \mathbb{F}_q^r, Q \mapsto (\alpha_1, \dots, \alpha_r)$ mit $Q(X) \equiv \alpha_j \pmod{P_j}$ für $1 \leq j \leq r$.

- Φ ist injektiv: Seien $Q_1, Q_2 \in V_f$ mit $\Phi(Q_1) = \Phi(Q_2)$. Dann gilt $Q_1(X) \equiv Q_2(X) \pmod{P_j}$, also $P_j \mid (Q_1 - Q_2)$ für $1 \leq j \leq r$. Also muss auch $f \mid (Q_1 - Q_2)$ gelten. Weil $\text{deg}(Q_1 - Q_2) < \text{deg } f$ ist $Q_1 = Q_2$.

- Φ ist surjektiv: Sei $(\alpha_1, \dots, \alpha_r) \in \mathbb{F}_q^r$, dann gibt es ein $Q \in \mathbb{F}_q[X]$ mit $Q \equiv \alpha_j \pmod{P_j}$ (chinesischer Restsatz).
 OBdA gilt $\deg Q < \deg f$, sonst Division mit Rest durch f . $Q^q \equiv \alpha_j^q = \alpha_j \equiv Q \pmod{P_j}$, also $Q^q \equiv Q \pmod{f}$ 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 . \square

Lemma 2.4. Sei $f \in \mathbb{F}_q[X]$, $\deg f = n$ und $X^{lq} \equiv q_{0,l} + q_{1,l}X + \dots + q_{n-1,l}X^{n-1} \pmod{f}$ 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 $b^{(1)}, \dots, b^{(r)}$ ein Basis des Eigenraumes von Q_f zum Eigenwert 1, $b^{(i)} = (b_0^{(i)}, \dots, b_{n-1}^{(i)})^t$ 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.

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

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

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

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

Berlekamp-Algorithmus: siehe Handout.

Bemerkung. • $\text{Ker}(Q_f - I_n)$ ist Eigenraum zum EW 1 von Q_f .

- $b^{(1)} = (1, 0, \dots, 0)^t \hat{=} Q(x) = 1 \in V_f, 1^q \equiv 1 \pmod{f}$.
- $b^{(1)}$ sicher $\in \text{Ker}(Q_f - I_n)$

- 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 2.5. *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.

$$P_i \mid d \quad \text{und} \quad P_j \nmid \frac{g}{d}.$$

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

$$\begin{aligned} B_s &\equiv \alpha_i \pmod{P_i} \\ B_s &\equiv \alpha_j \pmod{P_j}. \end{aligned}$$

Wir wissen: Es gibt ein Q_1 und ein $Q_2 \in V_f$ mit

$$\begin{aligned} Q &\equiv \alpha_i \pmod{P_i} \\ Q &\equiv \alpha_j \pmod{P_j} \end{aligned}$$

für verschiedene $\alpha_i \neq \alpha_j$.

$$Q = \sum_{s=1}^r \beta_s B_s.$$

Annahme:

$$\begin{aligned} B_s &\equiv \gamma_s \pmod{P_i} \\ B_s &\equiv \gamma_s \pmod{P_j} \end{aligned}$$

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

Also

$$\begin{aligned} Q &\equiv \sum \beta_s \gamma_s \pmod{P_i} \\ Q &\equiv \sum \beta_s \gamma_s \pmod{P_j}, \end{aligned}$$

Widerspruch zu $\alpha_i \neq \alpha_j$.

Falls P_i und P_j beim Schleifendurchlauf für dieses s und dieses α_i noch nicht getrennt sind $\Rightarrow P_i \mid B_s \alpha_i$, aber $P_i \nmid d$. $P_j \nmid B_s = \alpha_i$ (sonst $P_j \mid B_s - \alpha_j$ und $P_j \mid B_s - \alpha_i$ und somit $P_j \mid \alpha_j - \alpha_i$, eine Konstante $\neq 0$, Widerspruch).

Das heißt $P_j \nmid d$, also $P_j \nmid \frac{g}{d}$.

□

Kapitel 3

Grundbegriffe der Codierungstheorie

3.1 Einführung

- ISBN10 (International Standard Book Number):

– $\underbrace{3}$ - $\underbrace{540}$ $\underbrace{-64133-}$ $\underbrace{5}$
deutsch Springer Verlag Buch Prüfziffer
– bzw. 0-387-64133-5
– 3-540-97329-X

funktioniert modulo 11 (X=10).

- ISBN13 (= EAN):

– $\underbrace{978}$ 3540 64133 9
book land
– $\underbrace{49}$ 02778 91395 $\underbrace{3}$
Japan Prüfziffer

Überprüfung von EAN bzw. ISBN13:

$$(1, 3, 1, \dots, 3, 1, 3, 1) \cdot \begin{pmatrix} 9 \\ 7 \\ 8 \\ \vdots \end{pmatrix} \equiv 0 \pmod{10}.$$

Bei Überprüfung werden einfache Fehler erkannt:

- Eine Ziffer falsch:

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

- die meisten Ziffernstürze.

Nicht erkannt:

- Vertauschen zweier nebeneinanderliegender Ziffern, wenn sie kongruent $\pmod{5}$ sind:

$$3x + y \equiv x + 3y \pmod{10} \Leftrightarrow 2x \equiv 2y \pmod{10} \Leftrightarrow x \equiv y \pmod{5}.$$

Prüfziffer ist relativ billig: Informationsrate $\frac{12}{13}$.

- IBAN (International Bank Account Number): komische Manipulation, dann $\pmod{97}$.

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

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

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*.

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

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“), $m, n \in \mathbb{N}$. Eine Teilmenge C von A^n der Kardinalität $|C| = |A|^m$ heißt ein (n, m) -Blockcode. Eine bijektive Abbildung $E : A^m \rightarrow C$ heißt *Codierer* für C , die Umkehrabbildung heißt *Decodierer*.

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

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

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

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

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

3. $n = 6, m = 3$

Definition. Ein Codierer heißt *systematisch*, falls

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

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*

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

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

2. Das *Hamming-Gewicht* ist definiert als

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

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

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

Beweis. Offensichtlich gelten $d(x, y) \geq 0$, $d(x, y) = 0 \Leftrightarrow x = y$ und $d(x, y) = d(y, x)$.

Seien jetzt $x, y, z \in A^n$.

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

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

$$d(x, y) = \#(M \cup N) = \#M + \#N.$$

Außerdem

$$\#M \leq d(y, z)$$

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

$$\#N \leq d(x, y),$$

somit

$$d(x, z) = \#M + \#N \leq d(x, y) + d(y, z). \quad \square$$

Definition. Die *Minimaldistanz* $d(C)$ eines Blockcodes C ist als

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

definiert.

Beispiel. 1. Paritätscheck: $d(C) = 2$.

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

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. $d(x, y) \geq 2$, also $d(C) \geq 2$.

2. 3-facher Wiederholungscode:

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

3. $d(C) = 3$ (ohne Beweis). (Codewörter hinschreiben, alle Paare bilden.)

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

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

sodass

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

Bemerkung.

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

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

Proposition 3.1. Sei C ein (n, m) -Blockcode über A , $t \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:

1. Es gibt einen Fehlerprozessor F für C , der alle t -Bit-Fehler erkennt: $F(y) = ([y \in C], ?)$ für alle y und $d(y, C) = \min\{d(y, x) \mid x \in C\} \leq t$.
2. $d(C) \geq t + 1$.

Beweis. Angenommen, es existiert ein solcher Fehlerprozessor. Falls $d(C) \leq t$, so gibt es $z^1, z^2 \in C$ mit $d(z^1, z^2) \leq t$. z^2 könnte eine fehlerbehaftete Übertragung von z^1 sein, also

$$F(z^2) = \{\text{falsch}, ?\}.$$

Umgekehrt: $d(z^1, z^2) \geq t + 1$.

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

□

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. $d(C) \geq 2s + 1$

Beweisskizze. Für $x, y \in C$:

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

Bild! □

Satz 3.2. 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 $\in \{s + 1, \dots, s + t\}$ erkennt.
2. $d(C) \geq 2s + t + 1$

Beweisskizze. Für $x, y \in C$:

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

□

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^c “) heißt *linearer (n, m) -Code über \mathbb{F}_q* . Der Codierer $\mathbb{F}_q^m \rightarrow \mathbb{F}_q^n$ 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:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & & \\ \vdots & 0 & & \vdots \\ & \vdots & & \\ 0 & 0 & & 1 \\ 1 & 1 & & 1 \end{pmatrix} = \begin{pmatrix} I_7 \\ \mathbf{1}^t \end{pmatrix}$$

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 \iff Generatormatrix $= \begin{pmatrix} I_m \\ A \end{pmatrix}$ mit $A \in \mathbb{F}_q^{(n-m) \times m}$.

Proposition 3.3. Sei C ein linearer (n, m) -Code. Dann gibt es eine Matrix M , sodass

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

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

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

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

Es gilt $\text{Ker } F = C$. ($C \subseteq \text{Ker } F$ lt. Konstruktion. Im $F = \mathbb{F}_q^{n-m}$. Dimensionsformel: $\dim \text{Ker } F + \underbrace{\dim \text{Im } F}_{=n-m} = n$, somit $\dim \text{Ker } F = m \Rightarrow C = \text{Ker } F$.)

Eine Matrixdarstellung von F bzgl. Standardbasen ergibt die gewünschte Matrix.

Jede solche Matrix hat mindestens $n - m$ Zeilen, weil

$$\text{rank } M = n - \text{Ker } M = n - m. \quad \square$$

Definition. Eine Matrix mit den Eigenschaften aus der Proposition heißt *Prüfmatrix* (oder *Checkmatrix*) für C .

Beispiel. 1. Paritätscheck:

$$(1 \quad \dots \quad 1)$$

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 3.4. 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 $(-A \quad I_{n-m}) \in \mathbb{F}_q^{(n-m) \times m}$ eine Prüfmatrix für C .

Beweis.

$$\text{rank}(-A \quad I_{n-m}) = n - m \text{ wegen der Einheitsmatrix}$$

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

somit

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

also

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

Lt. Dimensionsformel

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

□

Proposition 3.5. Sei C ein linearer Code. Dann gilt

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

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

Beweis.

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

Da C linear ist, ist für $x, y \in C$ auch $x - y \in C$.

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

(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*?

Gegeben: $x \in \mathbb{F}_q^n$. Gesucht: $c \in C$ mit $d(c, x)$ minimal.

Standard-Tafel

q^m Spalten, q^{n-m} Zeilen. Jeder Eintrag ist ein Wort aus \mathbb{F}_q^n .

1. Zeile: alle Codewörter

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

Wähle ein x minimalen Gewichts, 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

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

Annahme: Empfangen ein x_{kj} .

Suche jenes $c \in C$ mit $d(x_{kj}, c)$ minimal, also $\text{wt}(x_{kj} - c)$ 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

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

Also: Die Standardtafel löst das Fehlerkorrekturproblem, aber sehr ineffizient.
Was ist das wirklich?

- Zeilen der Standardtafel: Nebenklassen $\text{mod } C$.
- 1. Element der Zeile: Element geringsten Gewichts aus der Nebenklasse („coset leader“).

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

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

Algorithmus Fehlerprozessor

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

Gesucht: $c \in C$ mit $d(x, y)$ minimal.

1. Vorberechnung: Bestimme für jede Nebenklasse ein Element x_j kleinsten Gewichts, setze $h_j = Mx_j$ („Hash-Wert“).
2. Berechnung: Suche j mit $Mx = h_j$. Gib $x - x_j$ zurück.

Korrektheit: siehe oben.

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

Beispiel. Betrachte $abcxyz$. Coset leaders:

$$7 \text{ Zeilen } \left\{ \begin{array}{l} 000000 \\ 100000 \\ \vdots \\ 000001 \end{array} \right.$$

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“.

Proposition 3.6. *Ein linearer Code hat genau dann Minimaldistanz $\geq d + 1$, wenn je d Spalten der Prüfmatrix linear unabhängig sind.*

Beweisskizze. Linearkombination von d Spalten entspricht Multiplikation von M mit Vektor mit Gewicht $\leq d$. Das wiederum entspricht Multiplikation mit Codevektor mit Gewicht $\leq d$. \square

Korollar 3.1. *Ein binärer linearer Code korrigiert 1-Bit Fehler genau dann, wenn alle Spalten der Prüfmatrix verschieden sind.*

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

Anhang

A1 Etwas lineare Algebra

In diesem Anhang sei V ein endlichdimensionaler Vektorraum über einem Körper K , $F : V \rightarrow V$ 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:*

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

Insbesondere ist g dadurch eindeutig definiert.

Beweis. Setze die Annihilatoren von F

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

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

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

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

Korollar A1.1. *Das Minimalpolynom teilt das charakteristische Polynom. Falls das Minimalpolynom vom Grad $\dim_K V$ ist, so gilt:*

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

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 . \square

Lemma A1.1. *Sei $r \in \mathbb{N}$, $\lambda \in K$ und J_r ein Jordanblock der Länge r zum Eigenwert λ . Dann ist das Minimalpolynom von J_r gleich $(X - \lambda)^r$.*

Beweis. $(X - \lambda)^r \in \text{Ann}(J_r)$ (siehe Lineare Algebra 2). Gibt es ein Polynom vom Grad $< r$, das J_r annihiliert, so sind $J_r^{r-1}v, \dots, J_r v, v$ für jeden Vektor v linear abhängig.

Für den r -ten Einheitsvektor ist das ein Widerspruch. (Nachrechnen!) \square

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

Satz A1.1. *Sei K ein Körper, V ein n -dimensionaler K -Vektorraum, $F : V \rightarrow V$ 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 $v, F(v), \dots, F^{n-1}(v)$ eine Basis von V ist.*

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

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

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

also ist $v, F(v), \dots, F^{n-1}(v)$ 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 ist. Setze $\text{Ann}(F, v) := \{g \in K[X] \mid g(F)(v) = 0\}$ für $v \in V$.

1. Behauptung: $\forall v \in V : \text{Ann}(F, v) \trianglelefteq K[X]$.
 - $0 \in \text{Ann}(F, v)$.
 - $\forall g_1, g_2 \in \text{Ann}(F, v) : (g_1 - g_2)(F)(v) = g_1(F)(v) - g_2(F)(v) = 0 - 0 = 0$.
 - $\forall h \in K[X] g \in \text{Ann}(F, v) : (hg)(F)(v) = h(F)(v)g(F)(v) = h(F)(v)0 = 0$.

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

2. Behauptung: für $j \in \{1, \dots, n\}$ gibt es ein v_j mit $\text{Ann}(F, v_j) = (f_j^{r_j})$.
 $\frac{f}{f_j}$ ist ein Polynom, 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 $f_j^{r_j} \in \text{Ann}(F, v_j)$.

Allerdings: $f_j^{r_j-1}(v_j) = \frac{f}{f_j}(F)(w_j) \neq 0$ laut Konstruktion von w_j . Also $f_j^{r_j-1} \notin \text{Ann}(F, v_j)$. Es folgt:

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

Aus der Eindeutigkeit der Primfaktorzerlegung folgt $g = f_j^{r_j}$.

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

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

also ist $gh \in \text{Ann}(F, v+w) = (g_1 h_1)$, 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 $gh_1 \in \text{Ann}(F, w) = (h_1 h_2)$. 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 ist h_2 konstant.

Analoges gilt für g_2 .

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

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