15. Vorlesung

- Primitive Polynome (Beispiel)
- Beispiel zur Konstruktion von $\mathrm{GF}(p)[x]/f(x)$ mit einem primitiven Polynom $f(x)$
  (Logarithmentafel)
- Struktur endlicher Körper
  - Rechnen in endlichen Körpern
  - Isomorphie von Körpern
  - Satz vom primitiven Element
- Anwendung: BCH-Codes verstehen ...
  - Primitive n-te Einheitswurzeln
  - Minimalpolynome

$\mathrm{GF}(p)[x]/f(x)$ für ein primitives Polynom $f(x)$

- Ist $f(x)$ ein primitives Polynom vom Grad k über $\mathrm{GF}(p)$, dann sind die Elemente von $\mathrm{GF}(p^k) \cong \mathrm{GF}(p)[x]/f(x)$:

$$
\begin{aligned}
&0\\
&x^0 = 1\\
&x \pmod{f(x)}\\
&x^2 \pmod{f(x)}\\
&\vdots\\
&x^{p^k-2} \pmod{f(x)}
\end{aligned}
$$

- Multiplikation in $\mathrm{GF}(p)[x]/f(x)$:

$$\boxed{x^i \pmod{f(x)} \otimes x^j \pmod{f(x)} = x^{i+j \pmod{p^k-1}} \pmod{f(x)}}$$

- Inverse Elemente:

$$\boxed{(x^i \pmod{f(x)})^{-1} = x^{p^k-1-i} \pmod{f(x)}}$$

Logarithmentafel für $GF(2)[x]/1 + x^3 + x^4$

i	α^i	$x^i \bmod 1 + x^3 + x^4$
0	α^0	1
1	α^1	x
2	α^2	x^2
3	α^3	x^3
4	α^4	$1 + x^3$
5	α^5	$1 + x + x^3$
6	α^6	$1 + x + x^2 + x^3$
7	α^7	$1 + x + x^2$
8	α^8	$x + x^2 + x^3$
9	α^9	$1 + x^2$
10	α^{10}	$x + x^3$
11	α^{11}	$1 + x^2 + x^3$
12	α^{12}	$1 + x$
13	α^{13}	$x + x^2$
14	α^{14}	$x^2 + x^3$

Bezeichnungen

- Bezeichung: $\alpha := x \pmod{f(x)}$
- Es sei $\mathrm{GF}(p^k) = \mathrm{GF}(p)[x]/f(x)$ ein endlicher Körper mit p^k Elementen, wobei $f(x)$ ein primitives Polynom vom Grad k über $\mathrm{GF}(p)$ ist.

  Es gilt dann

  $$\mathrm{GF}(p^k) = \{0\} \cup \{x^i \pmod{f(x)} \mid i = 0, 1, \ldots, p^k - 2\}$$

  und

  $$\alpha^i = x^i \pmod{f(x)},$$

  also

  $$\mathrm{GF}(p^k) = \{0\} \cup \{\alpha^i \mid i = 0, 1, \ldots, p^k - 2\}.$$

- Beispiel: $1 + x^3 + x^4$ ist ein primitives Polynom vom Grad 4

  $\mathrm{GF}(2^4) \cong \mathrm{GF}(2)[x]/1 + x^3 + x^4 = \{0\} \cup \{\alpha^i \mid i = 0, 1, \ldots, 14\}$

Rechnen in GF(p^k)

$$\mathrm{GF}(p^k) \setminus \{0\} = \{\alpha^i \mid i = 0, 1, \ldots, p^k - 2\}$$

- $0 \cdot 0 = 0$
- $0 \cdot \alpha^i = 0 \quad$ für $\quad i \in \{0, 1, \ldots, p^k - 2\}$
- $\alpha^i \cdot \alpha^j = \alpha^{(i+j) \bmod p^k - 1} \quad$ für $\quad i, j \in \{0, 1, \ldots, p^k - 2\}$
- $(\alpha^i)^{-1} = \alpha^{p^k - 1 - i} = \alpha^{-i}$ für $\quad i \in \{0, 1, \ldots, p^k - 2\}$
- $\alpha^i + \alpha^j \quad$ für $\quad i, j \in \{0, 1, \ldots, p^k - 2\}$

  kann man mit Hilfe einer Logarithmentafel berechnen:

i	α^i	x^i mod f(x)
0	1	1
1	α	x
2	α^2	x^2
$\vdots$	$\vdots$	$\vdots$

Satz vom primitiven Element

- Für jeden endlichen Körper GF(q) ist die multiplikative Gruppe zyklisch ist.

  In GF(q) gibt es also jeweils ein Element α mit

  $$GF(q) \setminus \{0\} = \langle \alpha \rangle = \{\alpha, \alpha^2, \ldots, \alpha^{q-1}\}.$$

  α wird ein primitives Element genannt. Es gilt $\alpha^{q-1} = 1$.

- Beispiel:

  2 ist ein primitives Element in $\mathbb{Z}_q$ für $q = 11$, $q = 13$, aber nicht für $q = 17$.

  x ist ein primitives Element in $GF(2)[x]/x^3 + x + 1$, aber nicht in $GF(2)[x]/x^4 + x^3 + x^2 + x + 1$.

  $x + 1$ ist ein primitives Element in $GF(2)[x]/x^4 + x^3 + x^2 + x + 1$.

- Ist $f(x)$ ein primitives Polynom über GF(p), dann ist x ein primitives Element in GF(p)$[x]/f(x)$.

Primitive n-te Einheitswurzeln

- Die Nullstellen von $x^n - 1$ in $\mathrm{GF}(p^k)$ nennt man die n-ten Einheitswurzeln in $\mathrm{GF}(p^k)$.
- Die n-ten Einheitswurzeln bilden eine zyklische Untergruppe der multiplikativen Gruppe von $\mathrm{GF}(p^k)$.
- Eine n-te Einheitswurzel in $\mathrm{GF}(p^k)$ heißt primitive n-te Einheitswurzel, wenn sie in der multiplikativen Gruppe von $\mathrm{GF}(p^k)$ ein Element der Ordnung n ist.
- Sei $\mathrm{ggT}(p, n) = 1$.
  $\mathrm{GF}(p^k)$ mit $n \mid (p^k - 1)$ $(k > 0,\ k \text{ minimal})$ ist der Körper mit kleinstem k, so dass $\mathrm{GF}(p^k)$ primitive n-te Einheitswurzeln enthält.

Minimalpolynome $m_{\alpha^i}(x)$

- Zu jedem Element von
  $\mathrm{GF}(p^k) \setminus \{0\} = \{\alpha^i \mid i = 0, 1, \ldots, p^k - 2\}$
  gibt es ein Minimalpolynom $m_{\alpha^i}(x)$ über $\mathrm{GF}(p)$.

- $m_{\alpha^i}(x) \in \mathrm{GF}(p)[x]$ ist irreduzibel über $\mathrm{GF}(p)$.

- $m_{\alpha^i}(x) = m_{\alpha^{i \cdot p^t}}(x)$ für alle $t \in \mathbb{N}$

- $m_{\alpha^i}(x)$ ist das normierte Polynom kleinsten Grades aus $\mathrm{GF}(p)[x]$, das α^i als Nullstelle hat.

- Berechnung der Minimalpolynome:

  $\alpha^i \in \mathrm{GF}(p^k) \setminus \{0\} \quad \Rightarrow \quad m_{\alpha^i}(x) = \prod_{j \in Z_i} (x - \alpha^j)$ mit

  $Z_i = \{i, ip, ip^2, \ldots, ip^\ell\}$;

  dabei bezeichnet ℓ die kleinste positive natürliche Zahl mit $i \cdot p^{\ell+1} \equiv i \pmod{p^k - 1}$.

Beispiel

$\mathrm{GF}(2^4) = \mathrm{GF}(2)[x]/1 + x^3 + x^4 \quad (1 + x^3 + x^4$ ist primitiv)

Minimalpolynome von α^0, α^1, ..., α^{14}:

$$
\begin{aligned}
Z_0 = \{0\} &\Rightarrow m_{\alpha^0}(x) = x - \alpha^0 \\
Z_1 = \{1,2,4,8\} &\Rightarrow m_{\alpha^1}(x) = (x-\alpha^1)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) \\
Z_1 = Z_2 = Z_4 = Z_8 &\Rightarrow m_{\alpha^1}(x) = m_{\alpha^2}(x) = m_{\alpha^4}(x) = m_{\alpha^8}(x) \\
Z_3 = \{3,6,12,9\} &\Rightarrow m_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) \\
Z_3 = Z_6 = Z_9 = Z_{12} &\Rightarrow m_{\alpha^3}(x) = m_{\alpha^6}(x) = m_{\alpha^9}(x) = m_{\alpha^{12}}(x) \\
Z_5 = \{5,10\} &\Rightarrow m_{\alpha^5}(x) = (x-\alpha^5)(x-\alpha^{10}) \\
Z_5 = Z_{10} &\Rightarrow m_{\alpha^5}(x) = m_{\alpha^{10}}(x) \\
Z_7 = \{7,14,13,11\} &\Rightarrow m_{\alpha^7}(x) = (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11}) \\
Z_7 = Z_{11} = Z_{13} = Z_{14} &\Rightarrow m_{\alpha^7}(x) = m_{\alpha^{11}}(x) = m_{\alpha^{13}}(x) = m_{\alpha^{14}}(x)
\end{aligned}
$$

Zur Berechnung der Minimalpolynome als Elemente von $\mathrm{GF}(2^4)[x]$ nutzt man die Logarithmentafel des Körpers $\mathrm{GF}(2^4) = \mathrm{GF}(2)[x]/1 + x^3 + x^4$.

Zerlegung von $x^{15} - 1$ in irreduzible Faktoren über GF(2)

- $m_{\alpha^0}(x) = x - \alpha^0$
- $m_{\alpha^1}(x) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) = x^4 + x^3 + 1$
- $m_{\alpha^3}(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = x^4 + x^3 + x^2 + x + 1$
- $m_{\alpha^5}(x) = (x - \alpha^5)(x - \alpha^{10}) = x^2 + x + 1$
- $m_{\alpha^7}(x) = (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11}) = x^4 + x + 1$
- $x^{15} - 1 =$
  $\underbrace{(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)\underbrace{(x^4+x+1)(x^4+x^3+1)}_{\text{primitive Polynome}}}_{\text{irreduzible Polynome}}$

- Da Minimalpolynome irreduzibel sind, kann man das kgV von Minimalpolynomen sehr leicht berechnen.

BCH-Codes

Sei α eine primitive n-te Einheitswurzel in $\mathrm{GF}(p^k)$:

$$\mathrm{GF}(p^k) \setminus \{0\} = \{\alpha^0, \alpha^1, \ldots, \alpha^{p^k-2}\}$$

Sei $\delta \in \mathbb{N}$, $\delta \leq n$, $b \in \mathbb{N}$, $b > 0$.

Ein zyklischer (n, k)-Linearcode $\mathcal{C}$ mit dem Generatorpolynom

$$g(x) = \mathrm{kgV}(m_{\alpha^b}(x),\ m_{\alpha^{b+1}}(x),\ , \ldots, m_{\alpha^{b+\delta-2}}(x))$$

wird **BCH-Code** der **Länge** n zur **Entwurfsdistanz** δ genannt.

Dabei bezeichnen $m_{\alpha^i}(x)$ für $i = b, b+1, \ldots, b+\delta-2$
die Polynome kleinsten Grades aus $\mathrm{GF}(p)[x]$,
die $\alpha^i \in \mathrm{GF}(p^k)$ als Nullstelle haben

(**Minimalpolynome** von $\alpha^i \in \mathrm{GF}(p^k)$).