

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

<http://www14.in.tum.de/lehre/2012WS/ds/>

Wintersemester 2012

Title: Meixner: test2 (04.12.2012)

Date: Tue Dec 04 13:50:22 CET 2012

Duration: 90:18 min

Pages: 42



Bemerkungen

- 4 Kongruenz modulo n definiert auf \mathbb{Z} eine Äquivalenzrelation $\sim_n: m \sim_n \ell : \iff m$ teilt $m - \ell$, und $[\ell]_n$ ist die Äquivalenzklasse von ℓ .
- 5 Auf der Menge aller Restklassen $[\ell]_n$ kann man Addition und Multiplikation wie folgt definieren

$$[\ell]_n +_n [m]_n := [\ell + m]_n, \quad [\ell]_n \cdot_n [m]_n := [\ell \cdot m]_n,$$

und erhält einen kommutativen Ring; er heißt der **Restklassenring \mathbb{Z} modulo n** und wird mit $\mathbb{Z}/(n)$ oder $\mathbb{Z}/n\mathbb{Z}$ oder \mathbb{Z}_n bezeichnet.

- 6 Die Abbildung $(\mathbb{Z}, +, \cdot) \rightarrow (\mathbb{Z}_n, +_n, \cdot_n), \ell \mapsto \text{„Rest der Division von } \ell \text{ durch } n\text{“}$ ist ein Ringhomomorphismus.



Restklassen können auch im Polynomring $K[x]$ (K ein Körper) gebildet werden.

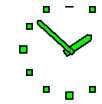
Definition 154

Sei $g \in K[x]$ ein Polynom, $\text{grad}(g) \geq 1$. Für jedes $f \in K[x]$ heißt die Menge

$$[f]_g := \{h \in K[x] : h - f \text{ ist durch } g \text{ teilbar}\}$$

die **Restklasse von f modulo g** .

Bemerkung: Wie in \mathbb{Z} gilt nun auch im Polynomring $K[x]$:



3.6 Restklassen in Polynomringen

3.6.1 Einführung und Definitionen

Der Begriff der Restklasse stammt ursprünglich aus der Teilbarkeitslehre in \mathbb{Z} ; $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring).

Definition 153

Sei n eine fest gewählte ganze Zahl $\neq 0$. Für jedes $\ell \in \mathbb{Z}$ heißt die Menge

$$[\ell]_n := \{m \in \mathbb{Z} : m - \ell \text{ ist durch } n \text{ teilbar}\}$$

die Restklasse von ℓ modulo n .

TUM Diskrete Strukturen ©Ernst W. Mayr 238/264 LEA

3.6 Restklassen in Polynomringen

3.6.1 Einführung und Definitionen

Der Begriff der Restklasse stammt ursprünglich aus der Teilbarkeitslehre in \mathbb{Z} ; $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring).

Definition 153

Sei n eine fest gewählte ganze Zahl $\neq 0$. Für jedes $\ell \in \mathbb{Z}$ heißt die Menge

$$[\ell]_n := \{m \in \mathbb{Z} : m - \ell \text{ ist durch } n \text{ teilbar}\}$$

die Restklasse von ℓ modulo n .

TUM Diskrete Strukturen ©Ernst W. Mayr 3.6 Restklassen in Polynomringen 238/264 LEA

Bemerkungen

- 1 Für $\ell, m \in \mathbb{Z}$ gilt:

$$m \in [\ell]_n \iff m \bmod n = \ell \bmod n.$$

Gilt $m \in [\ell]_n$, so schreibt man auch $m \equiv \ell \pmod{n}$ oder $m = \ell \pmod{n}$ und spricht „ m kongruent ℓ modulo n “.

- 2 Es gilt $[\ell]_n = \{\ell + kn : k \in \mathbb{Z}\} =: \ell + n\mathbb{Z} =: \ell + (n)$.
- 3 Da es genau n verschiedene Reste $0, 1, \dots, n-1$ gibt, gibt es auch genau n verschiedene Restklassen $[0]_n, [1]_n, \dots, [n-1]_n$.

Bemerkungen

- 4 Kongruenz modulo n definiert auf \mathbb{Z} eine Äquivalenzrelation $\sim_n: m \sim_n \ell : \iff m$ teilt $m - \ell$, und $[\ell]_n$ ist die Äquivalenzklasse von ℓ .
- 5 Auf der Menge aller Restklassen $[\ell]_n$ kann man Addition und Multiplikation wie folgt definieren

$$[\ell]_n +_n [m]_n := [\ell + m]_n, \quad [\ell]_n \cdot_n [m]_n := [\ell \cdot m]_n,$$

unabhängig vom Repräsentanten

und erhält einen kommutativen Ring; er heißt der Restklassenring \mathbb{Z} modulo n und wird mit $\mathbb{Z}/(n)$ oder $\mathbb{Z}/n\mathbb{Z}$ oder \mathbb{Z}_n bezeichnet.

- 6 Die Abbildung $(\mathbb{Z}, +, \cdot) \rightarrow (\mathbb{Z}_n, +_n, \cdot_n), \ell \mapsto$ „Rest der Division von ℓ durch n “ ist ein Ringhomomorphismus.

$$[\ell]_n = [\ell \bmod n]_n$$

wegen Kongruenz



Restklassen können auch im Polynomring $K[x]$ (K ein Körper) gebildet werden.

Definition 154

Sei $g \in K[x]$ ein Polynom, $\text{grad}(g) \geq 1$. Für jedes $f \in K[x]$ heißt die Menge

$$[f]_g := \{h \in K[x] : h - f \text{ ist durch } g \text{ teilbar}\}$$

die Restklasse von f modulo g .

Bemerkung: Wie in \mathbb{Z} gilt nun auch im Polynomring $K[x]$:



„Kongruenz modulo g “ definiert auf $K[x]$ eine Äquivalenzrelation $\sim_g: h \sim_g f \iff h - f$ ist durch g teilbar, und $[f]_g$ ist die Äquivalenzklasse von f .

Auf der Menge aller Restklassen $[f]_g$ kann man Addition und Multiplikation wie folgt definieren

$$[f]_g + [h]_g := [f + h]_g, \quad [f]_g \cdot [h]_g := [f \cdot h]_g,$$

und erhält einen kommutativen Ring; er heißt der Restklassenring $K[x]$ modulo g und wird mit $K[x]/(g)$ bezeichnet.



„Kongruenz modulo g “ definiert auf $K[x]$ eine Äquivalenzrelation $\sim_g: h \sim_g f \iff h - f$ ist durch g teilbar, und $[f]_g$ ist die Äquivalenzklasse von f .

Auf der Menge aller Restklassen $[f]_g$ kann man Addition und Multiplikation wie folgt definieren

$$[f]_g + [h]_g := [f + h]_g, \quad [f]_g \cdot [h]_g := [f \cdot h]_g,$$

und erhält einen kommutativen Ring; er heißt der Restklassenring $K[x]$ modulo g und wird mit $K[x]/(g)$ bezeichnet.



„Kongruenz modulo g “ definiert auf $K[x]$ eine Äquivalenzrelation $\sim_g: h \sim_g f \iff h - f$ ist durch g teilbar, und $[f]_g$ ist die Äquivalenzklasse von f .

Auf der Menge aller Restklassen $[f]_g$ kann man Addition und Multiplikation wie folgt definieren

$$[f]_g + [h]_g := [f + h]_g, \quad [f]_g \cdot [h]_g := [f \cdot h]_g,$$

und erhält einen kommutativen Ring; er heißt der Restklassenring $K[x]$ modulo g und wird mit $K[x]/(g)$ bezeichnet.





Satz 155

Sei $g \in K[x]$ ein Polynom, $d = \text{grad}(g) \geq 1$. Dann ist die Abbildung

$$(K[x]/(g), +, \cdot) \rightarrow (K[x]_d, +_g, \cdot_g), \quad [f]_g \mapsto \text{Rem}(f)$$

ein Ringisomorphismus, die Umkehrabbildung ist gegeben durch $r \mapsto [r]_g$.



Adobe Acrobat Professional window showing the slide content. The text and equation are identical to the first slide. The page number is 244/264.

Adobe Acrobat Professional window showing the second slide. The content includes Satz 135, an example, and a polynomial equation.

Satz 135
Zu je zwei Polynomen $a(x)$ und $b(x)$, $b \neq 0$, gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$, so dass

$$a(x) = q(x)b(x) + r(x) \text{ und } r = 0 \text{ oder } \text{grad}(r) < \text{grad}(b).$$

Beispiel 136
Im vorhergehenden Schema war das

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = \underbrace{(2x^2 - x + 3)}_{q(x)} \cdot \underbrace{(x^2 + x - 1)}_{b(x)} + \underbrace{(-3x + 6)}_{r(x)}$$

TUM Diskrete Strukturen ©Ernst W. Mayr 211/264 LEA



Adobe Acrobat Professional window showing the third slide. The content is identical to the first slide.

Satz 155
Sei $g \in K[x]$ ein Polynom, $d = \text{grad}(g) \geq 1$. Dann ist die Abbildung

$$(K[x]/(g), +, \cdot) \rightarrow (K[x]_d, +_g, \cdot_g), \quad [f]_g \mapsto \text{Rem}(f)$$

ein Ringisomorphismus, die Umkehrabbildung ist gegeben durch $r \mapsto [r]_g$.

TUM Diskrete Strukturen ©Ernst W. Mayr 244/264 LEA

Satz 155
 Sei $g \in K[x]$ ein Polynom, $d = \text{grad}(g) \geq 1$. Dann ist die Abbildung

$$(K[x]/(g), +, \cdot) \rightarrow (K[x]_d, +_g, \cdot_g), \quad [f]_g \mapsto \text{Rem}(f)$$

ein Ringisomorphismus, die Umkehrabbildung ist gegeben durch $r \mapsto [r]_g$.

TUM Diskrete Strukturen ©Ernst W. Mayr 3.6 Restklassen in Polynomringen 244/264 LEA

Beweis:
 Es gilt

$$[f]_g = [0]_g \iff g|f \iff \text{Rem}(f) = 0$$

$$[f]_g + [h]_g = [f+h]_g \mapsto \text{Rem}(f+h) = \text{Rem}(f) + \text{Rem}(h) = \text{Rem}(f) +_g \text{Rem}(h)$$

$$[f]_g \cdot [h]_g = [f \cdot h]_g \mapsto \text{Rem}(f \cdot h) = \text{Rem}(\text{Rem}(f) \cdot \text{Rem}(h)) = \text{Rem}(f) \cdot_g \text{Rem}(h).$$

Aus (1) - (3) folgt, dass obige Abbildung wohldefiniert, injektiv und ein Ringhomomorphismus ist; sie ist auch surjektiv, denn für $f \in K[x]_d$ ist $\text{Rem}(f) = f$.

TUM Diskrete Strukturen ©Ernst W. Mayr 245/264 LEA

Beweis:
 Es gilt

- $[f]_g = [0]_g \iff g|f \iff \text{Rem}(f) = 0$
- $[f]_g + [h]_g = [f+h]_g \mapsto \text{Rem}(f+h) = \text{Rem}(f) + \text{Rem}(h) = \text{Rem}(f) +_g \text{Rem}(h)$
- $[f]_g \cdot [h]_g = [f \cdot h]_g \mapsto \text{Rem}(f \cdot h) = \text{Rem}(\text{Rem}(f) \cdot \text{Rem}(h)) = \text{Rem}(f) \cdot_g \text{Rem}(h).$

Aus (1) - (3) folgt, dass obige Abbildung wohldefiniert, injektiv und ein Ringhomomorphismus ist; sie ist auch surjektiv, denn für $f \in K[x]_d$ ist $\text{Rem}(f) = f$.

TUM Diskrete Strukturen ©Ernst W. Mayr 3.6 Restklassen in Polynomringen 245/264 LEA

Satz 156
 Sei K ein Körper mit n Elementen, und sei $g \in K[x]$, $d = \text{grad}(g) \geq 1$. Dann besitzt $K[x]/(g)$ genau n^d Elemente.

Beweis:
 Nach Satz 155 ist $|K[x]/(g)| = |K[x]_d|$, und offensichtlich gilt $|K[x]_d| = n^d$.

Definition 157
 Ein Polynom $g \in K[x]$ heißt irreduzibel, falls $\text{grad}(g) \geq 1$ gilt und aus $g = g_1 \cdot g_2$ mit $g_1, g_2 \in K[x]$ stets $\text{grad}(g_1) = 0$ oder $\text{grad}(g_2) = 0$ folgt; ansonsten heißt g reduzibel.

TUM Diskrete Strukturen ©Ernst W. Mayr 246/264 LEA

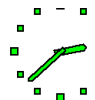


Satz 158

Sei $g \in K[x]$, $\text{grad}(g) \geq 1$. Dann gilt:

$K[x]/(g)$ ist ein Körper $\Leftrightarrow g$ ist irreduzibel.

Beweis:



Satz 158

Sei $g \in K[x]$, $\text{grad}(g) \geq 1$. Dann gilt:

$K[x]/(g)$ ist ein Körper $\Leftrightarrow g$ ist irreduzibel.

Beweis:

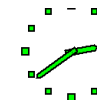
“ \Rightarrow ” Sei $K[x]/(g)$ ein Körper. Angenommen, g ist **nicht** irreduzibel. Dann gibt es $g_1, g_2 \in K[x]$ mit $g = g_1 \cdot g_2$ und $\text{grad}(g_1), \text{grad}(g_2) \geq 1$.

Da $d := \text{grad}(g) = \text{grad}(g_1) + \text{grad}(g_2)$, folgt $\text{grad}(g_1) < d$ und $\text{grad}(g_2) < d$.

Also gilt $[g_1]_g \neq [0]_g$ und $[g_2]_g \neq [0]_g$. Jedoch ist

$$[g_1]_g \cdot [g_2]_g = [g_1 g_2]_g = [g]_g = [0]_g,$$

d.h. $[g_1]_g$ und $[g_2]_g$ sind Nullteiler. In einem Körper gibt es jedoch keine Nullteiler (vgl. Satz 123).



Satz 158

Sei $g \in K[x]$, $\text{grad}(g) \geq 1$. Dann gilt:

$K[x]/(g)$ ist ein Körper $\Leftrightarrow g$ ist irreduzibel.

Beweis:

“ \Rightarrow ” Sei $K[x]/(g)$ ein Körper. Angenommen, g ist **nicht** irreduzibel. Dann gibt es $g_1, g_2 \in K[x]$ mit $g = g_1 \cdot g_2$ und $\text{grad}(g_1), \text{grad}(g_2) \geq 1$.

Da $d := \text{grad}(g) = \text{grad}(g_1) + \text{grad}(g_2)$, folgt $\text{grad}(g_1) < d$ und $\text{grad}(g_2) < d$.

Also gilt $[g_1]_g \neq [0]_g$ und $[g_2]_g \neq [0]_g$. Jedoch ist

$$[g_1]_g \cdot [g_2]_g = [g_1 g_2]_g = [g]_g = [0]_g,$$

d.h. $[g_1]_g$ und $[g_2]_g$ sind Nullteiler. In einem Körper gibt es jedoch keine Nullteiler (vgl. Satz 123).



Beweis (Forts.):

“ \Leftarrow ” Sei g irreduzibel, und sei $[f]_g \neq [0]_g$ gegeben.

$[f]_g \neq [0]_g$ bedeutet, dass f nicht durch g teilbar ist. Da g irreduzibel ist, sind f und g daher teilerfremd.

Somit existieren Polynome $p, q \in K[x]$ mit $pf + qg = 1$, und es folgt

$$\begin{aligned} [p]_g \cdot [f]_g &= [pf]_g = [1 - qg]_g = [1]_g - \underbrace{[qg]_g}_{=[0]_g} \\ &= [1]_g. \end{aligned}$$

Also ist $[p]_g = ([f]_g)^{-1}$.



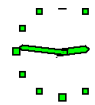


3.7 Konstruktion endlicher Körper

Satz 159

Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es einen endlichen Körper mit p^n Elementen; dieser wird mit $GF(p^n)$ bezeichnet ($GF = \text{Galois Field}$, nach *Evariste Galois* (1811–1832)).

Beweis:

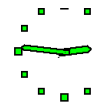


3.7 Konstruktion endlicher Körper

Satz 159

Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es einen endlichen Körper mit p^n Elementen; dieser wird mit $GF(p^n)$ bezeichnet ($GF = \text{Galois Field}$, nach *Evariste Galois* (1811–1832)).

Beweis:



3.7 Konstruktion endlicher Körper

Satz 159

Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es einen endlichen Körper mit p^n Elementen; dieser wird mit $GF(p^n)$ bezeichnet ($GF = \text{Galois Field}$, nach *Evariste Galois* (1811–1832)).

Beweis:

$n = 1$: $\mathbb{Z}_p = GF(p)$ ist ein Körper mit p Elementen.

$n > 1$: Sei $K = \mathbb{Z}_p$. Sei $y \in K[x]$ ein *irreduzibles* Polynom vom Grad n (zur Existenz eines solchen Polynoms: siehe Bemerkung unten).

□

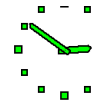


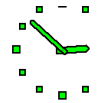
Satz 160

Je zwei endliche Körper mit p^n Elementen sind *isomorph*.

Beweis:

siehe geeignetes Textbuch zur Algebra oder Zahlentheorie, ebenfalls bzgl. der Existenz irreduzibler Polynome! □





Beispiel 161

Wir betrachten den Fall $K = \mathbb{Z}_3 = GF(3)$ und $p(x) = x^2 + 1$.

Der Ring $\mathbb{Z}_3[x]/(p)$ besteht also aus allen Polynomen in $\mathbb{Z}_3[x]$ vom Grad ≤ 1 :

$$\mathbb{Z}_3[x]/(p) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$$

Bemerkung zur Notation: Wir schreiben hier (und auch sonst) das Polynom f statt der Restklasse $[f]_p$.

Das Polynom p ist irreduzibel. Wieso?



Beispiel 162

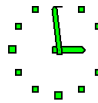
Für $K = \mathbb{Z}_2 = GF(2)$ und $p(x) = x^2 + x + 1$ gilt in ähnlicher Weise

$$\mathbb{Z}_2[x]/(p) = \{0, 1, x, x+1\}.$$

Für die Addition und Multiplikation modulo p ergibt sich

$+_p$	0	1	x	$x+1$	\cdot_p	0	1	x	$x+1$
0	0	1	x	$x+1$	0	0	0	0	0
1	1	0	$x+1$	x	1	0	1	x	$x+1$
x	x	$x+1$	0	1	x	0	x	$x+1$	1
$x+1$	$x+1$	x	1	0	$x+1$	0	$x+1$	1	x

Aus diesen beiden Tabellen folgt, dass $\mathbb{Z}_2[x]/(p)$ mit den angegebenen Verknüpfungen $+_p$ und \cdot_p einen Körper mit 4 Elementen bildet (den wir schon früher gesehen haben).



Beispiel 162

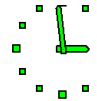
Für $K = \mathbb{Z}_2 = GF(2)$ und $p(x) = x^2 + x + 1$ gilt in ähnlicher Weise

$$\mathbb{Z}_2[x]/(p) = \{0, 1, x, x+1\}.$$

Für die Addition und Multiplikation modulo p ergibt sich

$+_p$	0	1	x	$x+1$	\cdot_p	0	1	x	$x+1$
0	0	1	x	$x+1$	0	0	0	0	0
1	1	0	$x+1$	x	1	0	1	x	$x+1$
x	x	$x+1$	0	1	x	0	x	$x+1$	1
$x+1$	$x+1$	x	1	0	$x+1$	0	$x+1$	1	x

Aus diesen beiden Tabellen folgt, dass $\mathbb{Z}_2[x]/(p)$ mit den angegebenen Verknüpfungen $+_p$ und \cdot_p einen Körper mit 4 Elementen bildet (den wir schon früher gesehen haben).



Beispiel 162

Für $K = \mathbb{Z}_2 = GF(2)$ und $p(x) = x^2 + x + 1$ gilt in ähnlicher Weise

$$\mathbb{Z}_2[x]/(p) = \{0, 1, x, x+1\}.$$

Für die Addition und Multiplikation modulo p ergibt sich

$+_p$	0	1	x	$x+1$	\cdot_p	0	1	x	$x+1$
0	0	1	x	$x+1$	0	0	0	0	0
1	1	0	$x+1$	x	1	0	1	x	$x+1$
x	x	$x+1$	0	1	x	0	x	$x+1$	1
$x+1$	$x+1$	x	1	0	$x+1$	0	$x+1$	1	x

Aus diesen beiden Tabellen folgt, dass $\mathbb{Z}_2[x]/(p)$ mit den angegebenen Verknüpfungen $+_p$ und \cdot_p einen Körper mit 4 Elementen bildet (den wir schon früher gesehen haben).





Beispiel 163

Für $K = \mathbb{Z}_2$ und $q(x) = x^2 + 1$ gilt wiederum

$$\mathbb{Z}_2[x]/(q) = \{0, 1, x, x+1\}.$$

Für die Addition und Multiplikation modulo q ergibt sich nunmehr jedoch

$+_q$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

\cdot_q	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

Aus der zweiten Tabelle folgt, dass $\mathbb{Z}_2[x]/(q) \setminus \{0\}$ bzgl. \cdot_q keine Gruppe bildet. Der Grund ist, dass q nicht irreduzibel ist.



3.8 Redundante Datenspeicherung und Fehlerkorrektur

Seien natürliche Zahlen k, t und s so gewählt, dass

$$k + 2t \leq 2^s - 1.$$

Sei weiter $K = GF(2^s)$, und seien $\alpha_0, \dots, \alpha_{k-1} \in K$. Wir fassen die α_i sowohl als Elemente von K als auch (in frei festzulegender, eindeutiger Weise) als *Binärwörter* der Länge s auf.

Sei weiter α ein primitives Element in $K = GF(2^s)$ (existiert nach Satz 127) und seien



$$g(x) := \prod_{i=1}^{2t} (x - \alpha^i),$$

$$c(x) := \sum_{i=0}^{k-1} c_i x^i, \text{ und}$$

$$d(x) = \sum_{i=0}^{k+2t-1} d_i x^i := g(x) \cdot c(x).$$

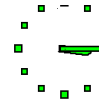
Wir sagen, dass der Vektor der Koeffizienten von $d(x)$ den Vektor (c_0, \dots, c_{k-1}) kodiert (Reed-Solomon-Code $RS(s, k, t)$).

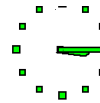


Satz 164

Für jedes $s \in \mathbb{N}$ und $k, t \in \mathbb{N}$ mit $k + 2t \leq 2^s - 1$ ist der Reed-Solomon-Code $RS(s, k, t)$ t -fehlerkorrigierend und $2t$ -fehlererkennend.

Das bedeutet, dass, falls bei der Übertragung des Vektors der d_i nicht mehr als $2t$ der d_i 's verändert werden, dies erkannt werden kann. Werden höchstens t der d_i 's verändert, so können die ursprünglichen d_i 's sogar rekonstruiert werden.





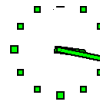
Beweis:

Sei (f_0, \dots, f_{k+2t-1}) der sich nach der Übertragung ergebende Code-Vektor, sei $e_i := f_i - d_i$ für $i = 0, \dots, k+2t-1$, und seien

$$e(x) := \sum_{i=0}^{k+2t-1} e_i x^i \text{ und } f(x) := \sum_{i=0}^{k+2t-1} f_i x^i.$$

Dann gilt $f(x) = d(x) + e(x)$, und es folgt

$$f(\alpha^i) = e(\alpha^i) \quad \text{für alle } 1 \leq i \leq 2t.$$

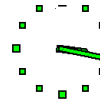


$$g(x) := \prod_{i=1}^{2t} (x - \alpha^i),$$

$$c(x) := \sum_{i=0}^{k-1} c_i x^i, \text{ und}$$

$$d(x) = \sum_{i=0}^{k+2t-1} d_i x^i := g(x) \cdot c(x).$$

Wir sagen, dass der Vektor der Koeffizienten von $d(x)$ den Vektor (c_0, \dots, c_{k-1}) kodiert (Reed-Solomon-Code $RS(s, k, t)$).



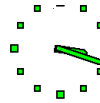
Beweis:

Sei (f_0, \dots, f_{k+2t-1}) der sich nach der Übertragung ergebende Code-Vektor, sei $e_i := f_i - d_i$ für $i = 0, \dots, k+2t-1$, und seien

$$e(x) := \sum_{i=0}^{k+2t-1} e_i x^i \text{ und } f(x) := \sum_{i=0}^{k+2t-1} f_i x^i.$$

Dann gilt $f(x) = d(x) + e(x)$, und es folgt

$$f(\alpha^i) = e(\alpha^i) \quad \text{für alle } 1 \leq i \leq 2t.$$



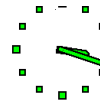
Beweis (Forts.):

In Matrixschreibweise sieht dies wie folgt aus:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{2(k+2t-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(k+2t-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t} & \alpha^{4t} & \alpha^{6t} & \dots & \alpha^{2t(k+2t-1)} \end{pmatrix} \cdot \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{k+2t-2} \\ e_{k+2t-1} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}.$$

Falls nur e_{i_1}, \dots, e_{i_r} ungleich 0 sind, fallen Spalten weg und es ergibt sich

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{2ti_1} \\ \alpha^{2i_1} & \alpha^{4i_1} & \dots & \alpha^{4ti_1} \\ \alpha^{3i_1} & \alpha^{6i_1} & \dots & \alpha^{6ti_1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2ti_1} & \alpha^{4ti_1} & \dots & \alpha^{2ti_1} \end{pmatrix} \cdot \begin{pmatrix} e_{i_1} \\ \vdots \\ e_{i_r} \end{pmatrix} = \begin{pmatrix} f(\alpha^{i_1}) \\ f(\alpha^{2i_1}) \\ f(\alpha^{3i_1}) \\ \vdots \\ f(\alpha^{2ti_1}) \end{pmatrix}.$$



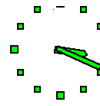
Beweis (Forts.):

In Matrixschreibweise sieht dies wie folgt aus:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{2(k+2t-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(k+2t-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t} & \alpha^{4t} & \alpha^{6t} & \dots & \alpha^{2t(k+2t-1)} \end{pmatrix} \cdot \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{k+2t-2} \\ e_{k+2t-1} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}.$$

Falls nur e_{i_1}, \dots, e_{i_r} ungleich 0 sind, fallen Spalten weg und es ergibt sich

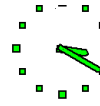
$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_r} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_r} \\ \alpha^{3i_1} & \alpha^{3i_2} & \dots & \alpha^{3i_r} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2ti_1} & \alpha^{2ti_2} & \dots & \alpha^{2ti_r} \end{pmatrix} \cdot \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_r} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}.$$



Beweis (Forts.):

Immer wenn die Anzahl r der Spalten \leq der Anzahl $2t$ der Zeilen ist, hat diese Matrix vollen Spaltenrang (Vandermonde-Matrix).

- Wenn $(e(\alpha^i) =) f(\alpha^i) = 0$ für $i = 1, \dots, 2t$, dann ist $e_i = 0$ für alle i eine Lösung, und zwar dann die einzige (Spaltenrang).
- Falls $\leq t$ Fehler aufgetreten sind, können wir entsprechende e_{i_j} eindeutig bestimmen (z.B. durch Probieren) und damit die d_i rekonstruieren.



Beweis (Forts.):

Immer wenn die Anzahl r der Spalten \leq der Anzahl $2t$ der Zeilen ist, hat diese Matrix vollen Spaltenrang (Vandermonde-Matrix).

- Wenn $(e(\alpha^i) =) f(\alpha^i) = 0$ für $i = 1, \dots, 2t$, dann ist $e_i = 0$ für alle i eine Lösung, und zwar dann die einzige (Spaltenrang).
- Falls $\leq t$ Fehler aufgetreten sind, können wir entsprechende e_{i_j} eindeutig bestimmen (z.B. durch Probieren) und damit die d_i rekonstruieren.

