WS 2003/04

Diskrete Strukturen I

Ernst W. Mayr

mayr@in.tum.de
Institut für Informatik
Technische Universität München

12-02-2003

Eigenschaften von Restklassenringen (Forts.)

Satz

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

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

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* $\mathrm{grad}(g_1), \mathrm{grad}(g_2) \geq 1$. *Da* $d := \mathrm{grad}(g) = \mathrm{grad}(g_1) + \mathrm{grad}(g_2)$, *folgt* $\mathrm{grad}(g_1) < d$ *und* $\mathrm{grad}(g_2) < d$. *Also gilt* $[g_1]_g \neq 0$ *und* $[g_2]_g \neq 0$. *Jedoch ist*

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

d.h. $[g_1]_g$ *und* $[g_2]_g$ *sind Nullteiler. In einem Körper gibt es jedoch keine Nullteiler (vgl. Satz 28 in 4.2).*

Eigenschaften von Restklassenringen (Forts.)

Satz

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

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

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* $\mathrm{grad}(g_1), \mathrm{grad}(g_2) \geq 1$. *Da* $d := \mathrm{grad}(g) = \mathrm{grad}(g_1) + \mathrm{grad}(g_2)$, *folgt* $\mathrm{grad}(g_1) < d$ *und* $\mathrm{grad}(g_2) < d$. *Also gilt* $[g_1]_g \neq 0$ *und* $[g_2]_g \neq 0$. *Jedoch ist*

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

d.h. $[g_1]_g$ *und* $[g_2]_g$ *sind Nullteiler. In einem Körper gibt es jedoch keine Nullteiler (vgl. Satz 28 in 4.2).*

Eigenschaften von Restklassenringen (Forts.)

Satz

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

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

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* $\mathrm{grad}(g_1), \mathrm{grad}(g_2) \geq 1$. *Da* $d := \mathrm{grad}(g) = \mathrm{grad}(g_1) + \mathrm{grad}(g_2)$, *folgt* $\mathrm{grad}(g_1) < d$ *und* $\mathrm{grad}(g_2) < d$. *Also gilt* $[g_1]_g \neq 0$ *und* $[g_2]_g \neq 0$. *Jedoch ist*

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

d.h. $[g_1]_g$ *und* $[g_2]_g$ *sind Nullteiler. In einem Körper gibt es jedoch keine Nullteiler (vgl. Satz 28 in 4.2).*

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

$[f]_g \neq 0$ 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

$$[p]_g \cdot [f]_g = [pf]_g = [1 - qg]_g = [1]_g - \underbrace{[qg]_g}_{=0}$$

$$= [1]_g \cdot$$

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

q. e. d.

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

$$[p]_g \cdot [f]_g = [pf]_g = [1 - qg]_g = [1]_g - \underbrace{[qg]_g}_{=0}$$

$$= [1]_g \cdot$$

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

q. e. d.

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

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

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

q. e. d.

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

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

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

q. e. d.

Konstruktion endlicher Körper

Satz

*Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es bis auf Isomorphie genau einen endlichen Körper mit p^n Elementen; dieser wird mit $GF(p^n)$ bezeichnet (GF = **G**alois **F**ield).*

Beweis.

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

$n > 1$: Sei $K = \mathbb{Z}_p$. Sei $g \in K[x]$ ein *irreduzibles* Polynom vom Grad n (zur Existenz eines solchen Polynoms: siehe Bemerkung unten).
Nach Satz 1 ist $K[x]/(g)$ ein Körper, und nach Korollar 17 hat $K[x]/(g)$ genau p^n Elemente. Die Eindeutigkeit wird im nächsten Satz gezeigt.

□

Konstruktion endlicher Körper

Satz

*Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es bis auf Isomorphie genau einen endlichen Körper mit p^n Elementen; dieser wird mit $GF(p^n)$ bezeichnet (GF = **G**alois **F**ield).*

Beweis.

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

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

Nach Satz 1 ist $K[x]/(g)$ ein Körper, und nach Korollar 17 hat $K[x]/(g)$ genau p^n Elemente. Die Eindeutigkeit wird im nächsten Satz gezeigt.

□

Konstruktion endlicher Körper

Satz

*Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es bis auf Isomorphie genau einen endlichen Körper mit p^n Elementen; dieser wird mit $GF(p^n)$ bezeichnet ($GF =$ **G**alois **F**ield).*

Beweis.

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

$n > 1$: Sei $K = \mathbb{Z}_p$. Sei $g \in K[x]$ ein *irreduzibles* Polynom vom Grad n (zur Existenz eines solchen Polynoms: siehe Bemerkung unten).
Nach Satz 1 ist $K[x]/(g)$ ein Körper, und nach Korollar 17 hat $K[x]/(g)$ genau p^n Elemente. Die Eindeutigkeit wird im nächsten Satz gezeigt.

□

Konstruktion endlicher Körper

Satz

*Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es bis auf Isomorphie genau einen endlichen Körper mit p^n Elementen; dieser wird mit $GF(p^n)$ bezeichnet (GF = **G**alois **F**ield).*

Beweis.

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

$n > 1$: Sei $K = \mathbb{Z}_p$. Sei $g \in K[x]$ ein *irreduzibles* Polynom vom Grad n (zur Existenz eines solchen Polynoms: siehe Bemerkung unten).
Nach Satz 1 ist $K[x]/(g)$ ein Körper, und nach Korollar 17 hat $K[x]/(g)$ genau p^n Elemente. Die Eindeutigkeit wird im nächsten Satz gezeigt.

□

Satz

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

Beweis.

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

Satz

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

Beweis.

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

Beispiel

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:

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

Das Polynom p ist irreduzibel. *Wieso?*

Beispiel

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:

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

Das Polynom p ist irreduzibel. *Wieso?*

Beispiel

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:

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

Das Polynom p ist irreduzibel. *Wieso?*

Beispiel

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	$x+1$
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

Beispiel

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	$x+1$
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

Beispiel

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	$x+1$
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

$\cdot_p$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	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).

$\cdot_p$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	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).

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

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

Beispiel

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

Beispiel

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.

$\cdot_q$	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.

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 $c_0, \ldots, c_{k-1} \in K$. Wir fassen die c_i sowohl als Elemente von K, aber auch (in festzulegender, eindeutiger Weise) als *Binärwörter der Länge* s auf.
Sei weiter α ein primitives Element in $K = GF(2^s)$ (existiert nach Satz 30 in 4.2), und seien

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 $c_0, \ldots, c_{k-1} \in K$. Wir fassen die c_i sowohl als Elemente von K, aber auch (in festzulegender, eindeutiger Weise) als *Binärwörter der Länge* s auf.

Sei weiter α ein primitives Element in $K = GF(2^s)$ (existiert nach Satz 30 in 4.2), und seien

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 $c_0, \ldots, c_{k-1} \in K$. Wir fassen die c_i sowohl als Elemente von K, aber auch (in festzulegender, eindeutiger Weise) als *Binärwörter der Länge* s auf.
Sei weiter α ein primitives Element in $K = GF(2^s)$ (existiert nach Satz 30 in 4.2), und seien

$$
\begin{aligned}
g(x) &:= \prod_{i=1}^{2t}(x-\alpha^i)\ , \\
c(x) &:= \sum_{i=0}^{k-1} c_i x^i\ , \text{ und} \\
d(x) = \sum_{i=0}^{k+2t-1} d_i x^i &:= g(x)\cdot c(x)\ .
\end{aligned}
$$

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

$$
\begin{aligned}
g(x) &:= \prod_{i=1}^{2t}(x-\alpha^i)\ , \\
c(x) &:= \sum_{i=0}^{k-1} c_i x^i\ , \text{ und} \\
d(x) = \sum_{i=0}^{k+2t-1} d_i x^i &:= g(x)\cdot c(x)\ .
\end{aligned}
$$

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

Satz

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.

Satz

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

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

In Matrixschreibweise sieht dies wie folgt aus:

Beweis

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

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

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

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

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

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

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

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

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

Wenn immer die Anzahl r der Spalten $\leq$ der Anzahl $2t$ der Zeilen ist, hat diese Matrix vollen Spaltenrang (*Vandermonde-Matrix*). *Wenn* $f(\alpha^i) = 0$ *für* $i = 1, \ldots, 2t$, *dann ist* $e_i = 0$ *für alle* i *eine Lösung, und zwar dann die einzige (Spaltenrang). Falls* $\leq 2t$ *Fehler aufgetreten sind, können wir entsprechende* e_{i_j} *eindeutig bestimmen und damit die* d_i *rekonstruieren.* *q. e. d.*

Wenn immer die Anzahl r der Spalten $\leq$ der Anzahl $2t$ der Zeilen ist, hat diese Matrix vollen Spaltenrang (*Vandermonde-Matrix*). *Wenn* $f(\alpha^i) = 0$ *für* $i = 1, \ldots, 2t$, *dann ist* $e_i = 0$ *für alle* i *eine Lösung, und zwar dann die einzige (Spaltenrang). Falls* $\leq 2t$ *Fehler aufgetreten sind, können wir entsprechende* e_{i_j} *eindeutig bestimmen und damit die* d_i *rekonstruieren.* *q. e. d.*