Endliche Körper

Seminar „Graphentheorie und Diskrete Mathematik“
Referent: Steffen Lohrke ii5105
SS 2005

Eine Abelsche Gruppe ist eine algebraische Struktur, die aus einer Menge K und einem zweistelligen Operatoren ($*$) besteht. Des weiteren muß gelten:

Abgeschlossenheit: $\forall\, a, b \in K:\ a * b \in K$

Assoziativgesetz: $\forall\, a, b, c \in K: a * (b * c) = (a * b) * c$

Existenz eines neutralen Elements e: $\forall\, a \in K: \exists\, e \in K: a * e = a$

Existenz eines inversen Elements b: $\forall\, a \in K: \exists\, b \in K: a * b = e$

Kommuntativgesetz: $\forall\, a, b \in K: a * b = b * a$

Beispiele:

$$(\mathbb{Z}, +)$$
$$(\mathbb{R}, +)$$
$$(\mathbb{R}\backslash\{0\}, *)$$
$$(\mathbb{R}^+, *)$$
$$(\mathbb{Q}\backslash\{0\}, *)$$
$$(\mathbb{Q}^+, *)$$

Abelsche Gruppe

Beispiele:

$(\mathbb{Z}, +)$
$(\mathbb{R}, +)$
$(\mathbb{R}\backslash\{0\}, *)$
$(\mathbb{R}^+, *)$
$(\mathbb{Q}\backslash\{0\}, *)$
$(\mathbb{Q}^+, *)$

Gegenbeispiele:

$(\mathbb{N}, +)$
$(\mathbb{R}^+, +)$
$(\mathbb{Z}\backslash\{0\}, *)$

Ein Ring ist eine algebraische Struktur, die aus einer Menge K und zwei zweistelligen Operatoren ($\otimes$ und $\oplus$) besteht. Desweiteren muß gelten:

(K, $\oplus$) ist eine Abelsche Gruppe, das neutrale Element wird als Null bezeichnet.

Abgeschlossenheit: $\forall\ a, b \in K:\ a \otimes b \in K$

Assoziativgesetz: $\forall\ a, b, c \in K: a \otimes (b \otimes c) = (a \otimes b) \otimes c$

Existenz eines neutralen Elements e: $\forall\ a \in K: \exists\ e \in K: a \otimes e = a$

Kommuntativgesetz: $\forall\ a, b \in K: a \otimes b = b \otimes a$

Distributivgesetz: $\forall\ a, b, c \in K:\ a \otimes (b \oplus c) = a \otimes b\ \oplus\ a \otimes c$

$$(b \oplus c) \otimes a = b \otimes a\ \oplus\ c \otimes a$$

Beispiele:

$$(\mathbb{R}, +, *)$$
$$(\mathbb{Q}, +, *)$$
$$(\mathbb{Z}, +, *)$$

Beispiele:

$(\mathbb{R}, +, *)$
$(\mathbb{Q}, +, *)$
$(\mathbb{Z}, +, *)$

Gegenbeispiele:

$(\mathbb{N}_0, +, *)$
$(\mathbb{R}^+, +, *)$

Ein Körper ist eine algebraische Struktur, die aus einer Menge K und zwei zweistelligen Operatoren ($\otimes$ und $\oplus$) besteht. Desweiteren muß gelten:

$(K, \oplus)$ ist eine Abelsche Gruppe, das neutrale Element wird als Null bezeichnet.

$(K\backslash\{0\},\otimes)$ ist eine Abelsche Gruppe, das neutrale Element wird als Eins bezeichnet.

Distributivgesetz: $\forall$ a, b, c $\in$ K: $a \otimes (b \oplus c) = a \otimes b \;\oplus\; a \otimes c$

$$(b \oplus c) \otimes a = b \otimes a \;\oplus\; c \otimes a$$

Beispiele:

$$(\mathbb{R}, +, *)$$
$$(\mathbb{Q}, +, *)$$

Beispiele:

$(\mathbb{R}, +, *)$
$(\mathbb{Q}, +, *)$

Gegenbeispiele:

$(\mathbb{N}_0, +, *)$
$(\mathbb{Z}, +, *)$
$(\mathbb{R}^+, +, *)$

Beispiele:

$(\mathbb{R}, +, *)$
$(\mathbb{Q}, +, *)$

Gegenbeispiele:

$(\mathbb{N}_0, +, *)$
$(\mathbb{Z}, +, *)$
$(\mathbb{R}^+, +, *)$

In Körpern kann man addieren, multiplizieren, subtrahieren und dividieren.

Endlicher Körper

Ein endlicher Körper ist ein Körper, bei dem
die Anzahl der Elemente der Menge K endlich ist.

Endlicher Körper

Ein endlicher Körper ist ein Körper, bei dem
die Anzahl der Elemente der Menge K endlich ist.

Endliche Körper werden auch Galoiskörper (Galois field) genannt.

Evariste Galois 1811-1832

Beispiel 1:

Die Menge der Restklassen $\mathbb{Z}_2$ bilden mit der Addition und Multiplikation den Körper GF(2).

$\mathbb{Z}_2 = \{ [0]_2 , [1]_2 \}$

$+_2$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	0	0
1	0	1

Beispiel 2:

Die Menge der Restklassen $\mathbb{Z}_3$ bilden mit der Addition und Multiplikation den Körper GF(3).

$\mathbb{Z}_3 = \{ [0]_3 , [1]_3 , [2]_3 \}$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Gegenbeispiel:

Die Menge der Restklassen $\mathbb{Z}_4$ bilden mit der Addition und Multiplikation keinen Körper.

$\mathbb{Z}_4 = \{ [0]_4, [1]_4, [2]_4, [3]_4 \}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$*_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Gegenbeispiel:

Die Menge der Restklassen $\mathbb{Z}_4$ bilden mit der Addition und Multiplikation keinen Körper.

$\mathbb{Z}_4 = \{ [0]_4 , [1]_4 , [2]_4 , [3]_4 \}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$*_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Lemma:

In jedem Körper K gilt: $\forall\, a \in K$: $a * 0 = 0 * a = 0$

Lemma:

In jedem Körper K gilt: $\forall\, a \in K{:}\quad a * 0 = 0 * a = 0$

Beweis: $0 + (a * 0) = a * 0 = a * (0 + 0) = a * 0 + a * 0$

$\Rightarrow\; 0 = a * 0$

Lemma:

In jedem Körper K gilt: $\forall\, a \in K: \quad a * 0 = 0 * a = 0$

Beweis: $0 + (a * 0) = a * 0 = a * (0 + 0) = a * 0 + a * 0$

$\Rightarrow\; 0 = a * 0$

Lemma:

In jedem Körper K gilt: $\forall\, a, b \in K: \quad a * b = 0 \;\Rightarrow\; a = 0 \vee b = 0$

Lemma:

In jedem Körper K gilt: $\forall\, a \in K{:}\quad a * 0 = 0 * a = 0$

Beweis: $0 + (a * 0) = a * 0 = a * (0 + 0) = a * 0 + a * 0$

$\Rightarrow\ 0 = a * 0$

Lemma:

In jedem Körper K gilt: $\forall\, a, b \in K{:}\quad a * b = 0 \ \Rightarrow\ a = 0 \vee b = 0$

Beweis: Wenn $a \neq 0$, dann existiert auch a^{-1}.

$b = 1 * b = a^{-1} * a * b = a^{-1} * 0 = 0$

$\Rightarrow\ b = 0$

Satz:

Bezeichnet man mit $+_n$ und $*_n$ die Addition bzw. die Multiplikation modulo n, so gilt:

$$(\mathbb{Z}_n, +_n, *_n) \text{ ist ein Körper} \quad \Rightarrow \quad n \text{ ist Primzahl}$$

Satz:

Bezeichnet man mit $+_n$ und $*_n$ die Addition bzw. die Multiplikation modulo n, so gilt:

$$(\mathbb{Z}_n, +_n, *_n) \text{ ist ein Körper} \quad \Leftrightarrow \quad n \text{ ist Primzahl}$$

Satz:

In jedem endlichen Körper K gibt es mindestens ein Element $a \in K\backslash\{0\}$ mit $K\backslash\{0\} = \{a^0, a^1, \ldots, a^{|K|-2}\}$.

Beispiele:

GF(3):

$2^0 = 1$
$2^1 = 2$

GF(7):

$3^0 = 1$	$5^0 = 1$
$3^1 = 3$	$5^1 = 5$
$3^2 = 2$	$5^2 = 4$
$3^3 = 6$	$5^3 = 6$
$3^4 = 4$	$5^4 = 2$
$3^5 = 5$	$5^5 = 3$

Neben den schon bekannten endlichen Körpern mit p Elementen, gibt es weitere endliche Körper mit p^k Elementen (p = Primzahl, $k \in \mathbb{N}$).

Neben den schon bekannten endlichen Körpern mit p Elementen, gibt es weitere endliche Körper mit p^k Elementen (p = Primzahl, $k \in \mathbb{N}$).

Ein endlicher Körper mit p^k Elementen kann mit Hilfe von Polynomen konstruiert werden:

$$\sum_{i=0}^{k-1} a_i x^i \quad \text{mit } a_i \in \mathbb{Z}_p$$

Außerdem wird ein irreduzibles Polynom vom Grad k benötigt.

Menge aller Polynome mit Koeffizienten in K:

$$K[x] := \left\{ \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}_0 ,\ a_i \in K \text{ und } a_n \neq 0 \text{ oder } n = 0 \right\}$$

Definition:

Ein Polynom $p(x) \in K[x]$ mit $p(x) \neq 0$ heißt irreduzibel über K, falls gilt:

$p(x) = f(x) * g(x)$ mit $f(x), g(x) \in K[x] \Rightarrow \text{grad}(f)=0$ oder $\text{grad}(g)=0$.

Beispiel:

$$(\mathbb{Z}_2[x]_{p(x)}, +_{p(x)}, *_{p(x)}) \quad \text{mit } p(x) = x^3 + x^2+1$$

$+_{x^3+x^2+1}$	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	x+1	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	x+1	0	1	x^2+x	x^2+x+1	x^2	x^2+1
x+1	x+1	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	x+1
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	x+1	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	x+1	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	x+1	x	1	0

fhwedel UNIVERSITY OF APPLIED SCIENCES

Beispiel (Fortsetzung):

$$(\mathbb{Z}_2[x]_{p(x)}, +_{p(x)}, *_{p(x)}) \quad \text{mit } p(x) = x^3 + x^2+1$$

$*_{x^3+x^2+1}$	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	x^2+1	x^2+x+1	1	x+1
x+1	0	x+1	x^2+x	x^2+1	1	x	x^2+x+1	x^2
x^2	0	x^2	x^2+1	1	x^2+x+1	x+1	x	x^2+x
x^2+1	0	x^2+1	x^2+x+1	x	x+1	x^2+x	x^2	1
x^2+x	0	x^2+x	1	x^2+x+1	x	x^2	x+1	x^2+1
x^2+x+1	0	x^2+x+1	x+1	x^2	x^2+x	1	x^2+1	x

Satz:

Sei K ein endlicher Körper und p(x) ein Polynom in K[x].
Dann gilt:

$(K[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ ist ein Körper $\Rightarrow$ p(x) ist irreduzibel über K[x].

Satz:

Sei K ein endlicher Körper und p(x) ein Polynom in K[x].
Dann gilt:

$(K[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ ist ein Körper $\Leftrightarrow$ p(x) ist irreduzibel über K[x].

Satz:

In jedem enlichen Körper K gibt es mindestens ein Element $\alpha \in K\backslash\{0\}$ mit $K\backslash\{0\} = \{\alpha^0, \alpha^1, \dots, \alpha^{|K|-2}\}$.

Beispiel: $(\mathbb{Z}_3[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ mit $p(x) = x^3 + x^2+1$

ord	Polynomdarstellung	Tupeldarstellung
0	0	000
α^0	1	100
α^1	x	010
α^2	x^2	001
α^3	$1 + x^2$	101
α^4	$1 + x + x^2$	111
α^5	$1 + x$	110
α^6	$x + x^2$	011

Satz:

Für ein $n \in \mathbb{N}$ gibt es genau einen Körper mit n Elementen, wenn $n = p^k$ für eine Primzahl p und ein $k \in \mathbb{N}$. Sind K_1 und K_2 zwei endliche Körper mit $|K_1| = |K_2|$, so gilt $K_1 \cong K_2$.

Das Reed-Solomon-Code *RS(s,k,t)* Verfahren ermöglicht es (durch hinzufügen von Zusatzinformationen) aus einen fehlerhaften Datensatz den korrekten Datensatz zu rekonstruieren.

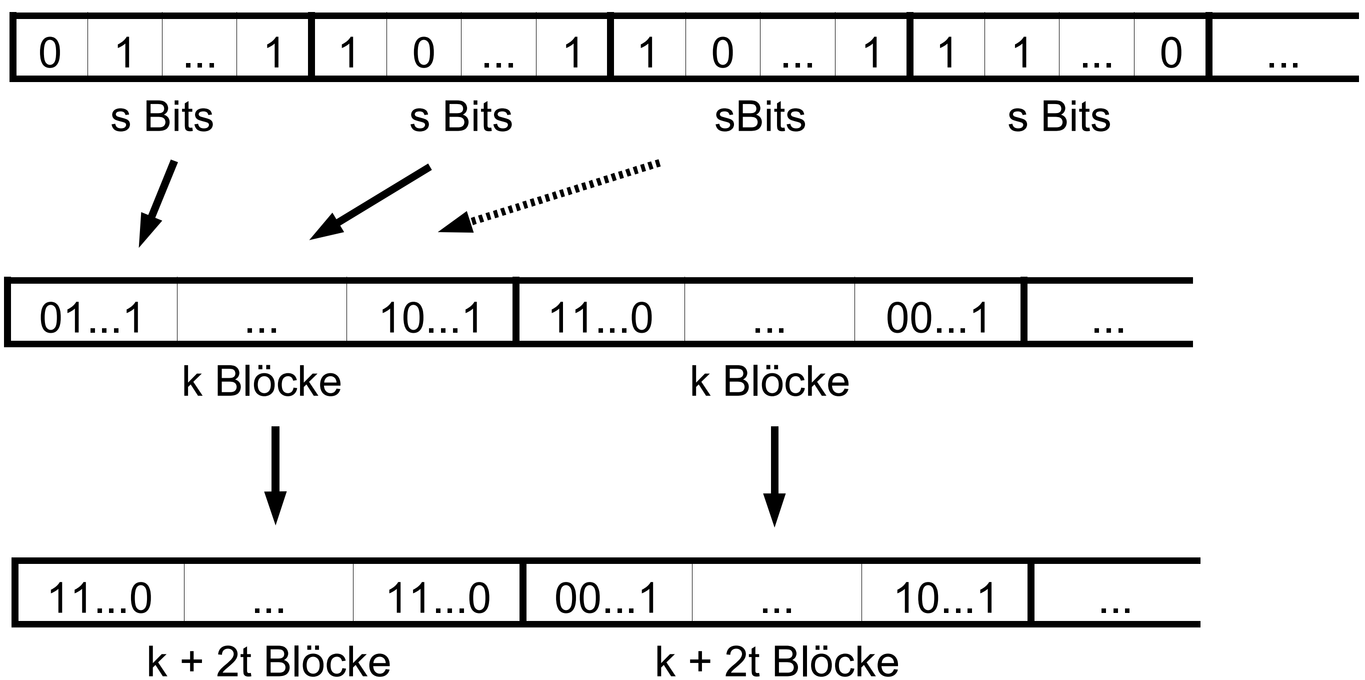
Die Parameter s, k und t sind natürliche Zahlen, die relativ frei festgelegt werden können. Es muß jedoch gelten:

$$k + 2t \leq 2^s$$

Das Verfahren kann t Fehler korrigieren und 2t Fehler erkennen.

Aus der Sequenz der Daten-Bits werden s-Bits zu einem Block zusammengefasst.

Aus k Blöcken werden aus s-Bits bestehende k + 2t Blöcke erzeugt.



Jede mögliche Bitfolge in einem Block wird auf einem Element aus dem endlichen Körper $GF(2^s)$ bijektiv abgebildet und die k zusammengefassten Blöcke werden nummeriert. Die k Blöcke können also als eine Folge von Elementen aus $GF(2^s)$ dargestellt werden:

$$c_1, \ldots, c_i, \ldots c_k \qquad \text{mit } c_i \in GF(2^s)$$

Daraus wird ein Polynom in x vom Grad k-1 erzeugt:

$$c(x) := \sum_{i=0}^{k-1} c_{i+1} x^i$$

Außerdem wird folgendes Polynom 2t-ten Grades benötigt:

$$g(x) := (x-\alpha) * (x-\alpha^2) * \ldots * (x-\alpha^{2t})$$

(α entspricht dem primitiven Element aus $GF(2^s)$)

Durch die Multiplikation vom c(x) und g(x) entsteht das Polynom d(x):

$$d(x) := c(x) * g(x)$$

Das Polynom d(x) hat daher den Grad 2t+k−1. Die Koeffizienten sind ebenfalls Elemente aus GF(2^s).

$$d(x) = \sum_{i=0}^{2t+k-1} d_{i+1} x^i$$

Bildet man die Koeffizienten d_i auf die entsprechende Bitfolge ab, so ergibt sich der kodierte Datensatz.

Aus den eingelesenen Daten kann das Polynom f(x) konstruiert werden.

$$f(x) = \sum_{i=0}^{2t+k-1} f_{i+1}x^i$$

Für den Fall, dass keine Fehler aufgetreten sind, ist f(x) identisch mit d(x) und durch dividieren mit g(x) erhält man die Ursprünglichen Daten.

Fehlererkennung (maximal 2t Koeffizienten fehlerhaft):

$$f(\alpha^1) = 0,\ f(\alpha^2) = 0,\ \ldots\ ,\ f(\alpha^{2t}) = 0$$

Stimmt eine oder mehrere dieser Gleichungen nicht liegt mindestens ein Fehler vor.

Für die Fehlerkorrektion nimmt man an, dass f(x) = d(x) + e(x) ist.

$$e(x) = \sum_{i=0}^{2t+k-1} e_{i+1} x^i$$

Ein Koeffizient f_i ist fehlerhaft, wenn $e_i \neq 0$ ist. Unter der Annahme, dass bekannt ist welche e_i's ungleich Null sind können diese mit Hilfe folgender Matrix berechnet werden:

$$\begin{pmatrix} \alpha^{i_1-1} & \alpha^{i_2-1} & \dots & \alpha^{i_r-1} \\ \alpha^{2(i_1-1)} & \alpha^{2(i_2-1)} & \dots & \alpha^{2(i_r-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2t(i_1-1)} & \alpha^{2t(i_2-1)} & \dots & \alpha^{2t(i_r-1)} \end{pmatrix} * \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_r} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}$$

$i_1, i_2, \dots, i_r$: Indizes der e_i's ungleich Null

Durch Subtrahieren der errechneten e_i's von den entsprechenden f_i's ergeben sich die korrekten d_i's.

Diskrete Strukturen Band 1
Angelika Steger
Springer-Verlag

Vorlesungsskript „Diskrete Mathematik“
von Prof. Dr. Rainer Lang (Handout)

Vorlesungsfolien „Diskrete Mathematik“
von Prof. Dr. Sebastian Iwanowski
http://www.fh-wedel.de/~iw

Vorlesungsskript „Einführung in Kanalcodierungsverfahren“
von Dr. Peter Stammnitz
http://iphome.hhi.de/stammnitz/ (nicht mehr online)

http://www.galois-group.net/

Fragen ???