Script generated by TTT

Title: Esparza: Diskrete Strukturen (06.02.2014)

Date: Thu Feb 06 10:15:17 CET 2014

Duration: 63:20 min

Pages: 32

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem: Verschlüsseln (Vereinfacht!)

  Um eine chiffrierte Nachricht an einen Teilnehmer B mit öffentlichem Schlüssel (n, c) zu senden:

  1. Zerlege die Nachricht so in Blöcke, dass jeder Block durch eine Zahl $m < n$ dargestellt werden kann (e.g. ASCII codes).
  2. Berechne für jeden Block das Element $x = m^c$ in der Gruppe $\mathbb{Z}_n^*$. Die Chiffrierung des Blocks ist die Zahl x.
  3. Schicke die Chiffrierungen x_1, x_2, x_3 … der Blöcke an B.

7

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebraische Strukturen

- Das RSA Kryptosystem
  - Das populärste asymmetrische Kryptosystem.
  - Benannt nach Rivest, Shamir, und Adleman (ähnliche Methode von Cocks wurde geheim gehalten).
  - Die Schlüssel sind (sehr) große Zahlen.
  - Die Verfahren für Ver- und Entschlüsselung basieren auf Zahlentheorie.

5

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Ka…n

- Sy…
  - Sender und Empfänger verwenden zum Ver- und Entschlüsseln einen einzigen, nur ihnen bekannten geheimen Schlüssel.
  - Die Sicherheit der Kommunikation hängt von der sicheren Aufbewahrung der geheimen Schlüssel ab.
  - Problem: Man braucht einen Schlüssel, um zu kommunizieren, aber man muss kommunizieren, um sich auf einen Schlüssel zu einigen …

3

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebra; Gruppen

- Zyklische Gruppen

  Definition: Ein Isomorphismus zwischen zwei Gruppen $\langle S_1, \circ_1 \rangle$ und $\langle S_2, \circ_2 \rangle$ ist eine Bijektion $f: S_1 \to S_2$ gibt mit $f(a \circ_1 b) = f(a) \circ_2 f(b)$ für alle $a, b \in S_1$.

  Zwei Gruppen sind isomorph wenn es ein Isomorphismus zwischen ihnen gibt.

  Beispiel: Die Bijektion $\{0, \dots, 3\} \to \{1, \dots, 4\}$ mit $0 \mapsto 1$, $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$ ist ein Isomorphismus zwischen $\langle \mathbb{Z}_4, +_4 \rangle$ und $\langle \mathbb{Z}_5 \setminus \{0\}, *_5 \rangle$.

Kapitel V – Algebra; Gruppen

- Zyklische Gruppen

  Definition: Ein Isomorphismus zwischen zwei Gruppen $\langle S_1, \circ_1 \rangle$ und $\langle S_2, \circ_2 \rangle$ ist eine Bijektion $f: S_1 \to S_2$ gibt mit $f(a \circ_1 b) = f(a) \circ_2 f(b)$ für alle $a, b \in S_1$.

  Zwei Gruppen sind isomorph wenn es ein Isomorphismus zwischen ihnen gibt.

  Beispiel: Die Bijektion $\{0, \dots, 3\} \to \{1, \dots, 4\}$ mit $0 \mapsto 1$, $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$ ist ein Isomorphismus zwischen $\langle \mathbb{Z}_4, +_4 \rangle$ und $\langle \mathbb{Z}_5 \setminus \{0\}, *_5 \rangle$.

33

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

4^6

$a \circ_1 b = c$

$f(a) \circ_2 f(b) = f(c)$

$4 *_5 4 *_5 4 *_5 4 \cdot$

- Zyklische Gruppen

Satz: Sei $G = \langle S, \circ \rangle$ eine zyklische Gruppe.

(1) Ist S unendlich, dann ist G isomorph zu $\langle \mathbb{Z}, + \rangle$.

(2) Ist S endlich, dann ist G isomorph zu $\langle \mathbb{Z}_{|S|}, +_{|S|} \rangle$.

Beweis: (1) Sei G zyklisch und unendlich.

Es existiert $a \in S$ mit $S = \{a^i \mid i \in \mathbb{Z}\}$.

Wir zeigen: Die Abbildung $f: \mathbb{Z} \to S$ definiert durch $f(i) = a^i$ ist ein Isomorphismus zwischen G und $\langle \mathbb{Z}, + \rangle$:

- Zyklische Gruppen

Beweis (Fort.):

- f ist surjektiv. Folgt aus der Definition einer zyklischen Gruppe.
- f ist injektiv. Wäre f nicht injektiv, dann gäbe es i, j mit $i > j$ und $a^i = a^j$. Dann wäre $a^{i-j} = e$ und somit $S \subseteq \{a^0, \ldots, a^{i-j-1}\}$, im Widerspruch zur Annahme, dass S unendlich ist.
- $\forall i, j \in \mathbb{Z} : f(i + j) = f(i) \circ f(j)$

  Es gilt: $f(i + j) = a^{i+j} = a^i \circ a^j = f(i) \circ f(j)$

Kapitel V – Algebra; Gruppen

- Zyklische Gruppen

Satz: Sei $G = \langle S, \circ \rangle$ eine zyklische Gruppe.

(1) Ist S unendlich, dann ist G isomorph zu $\langle \mathbb{Z}, + \rangle$.

(2) Ist S endlich, dann ist G isomorph zu $\langle \mathbb{Z}_{|S|}, +_{|S|} \rangle$.

Beweis: (1) Sei G zyklisch und unendlich.

Es existiert $a \in S$ mit $S = \{a^i \mid i \in \mathbb{Z}\}$.

Wir zeigen: Die Abbildung $f: \mathbb{Z} \to S$ definiert durch $f(i) = a^i$ ist ein Isomorphismus zwischen G und $\langle \mathbb{Z}, + \rangle$:

34

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebra; Gruppen

- Zyklische Gruppen

Beweis (Fort.):

- f ist surjektiv. Folgt aus der Definition einer zyklischen Gruppe.
- f ist injektiv. Wäre f nicht injektiv, dann gäbe es i, j mit $i > j$ und $a^i = a^j$. Dann wäre $a^{i-j} = e$ und somit $S \subseteq \{a^0, \ldots, a^{i-j-1}\}$, im Widerspruch zur Annahme, dass S unendlich ist.
- $\forall i, j \in \mathbb{Z} : f(i + j) = f(i) \circ f(j)$

  Es gilt: $f(i + j) = a^{i+j} = a^i \circ a^j = f(i) \circ f(j)$

35

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebra; Gruppen

- Zyklische Gruppen

  Beweis (Fort.):

  (2) Sei G zyklisch und endlich mit $|G| = m$.

  Analog zu (1):

  Es existiert $a \in S$ mit $S = \{a^0, a^1, \dots, a^{m-1}\}$.

  Wir zeigen wie in (1): Die Abbildung $f: \{0,1, \dots, m-1\} \to S$ definiert durch $f(i) = a^i$ ist ein Isomorphismus zwischen G und $\langle \mathbb{Z}_m, +_m \rangle$.

Kapitel V – Algebra; Gruppen

- Symmetrische Gruppen

  Definition: Eine Permutation ist eine bijektive Abbildung einer endlichen Menge auf sich selbst.

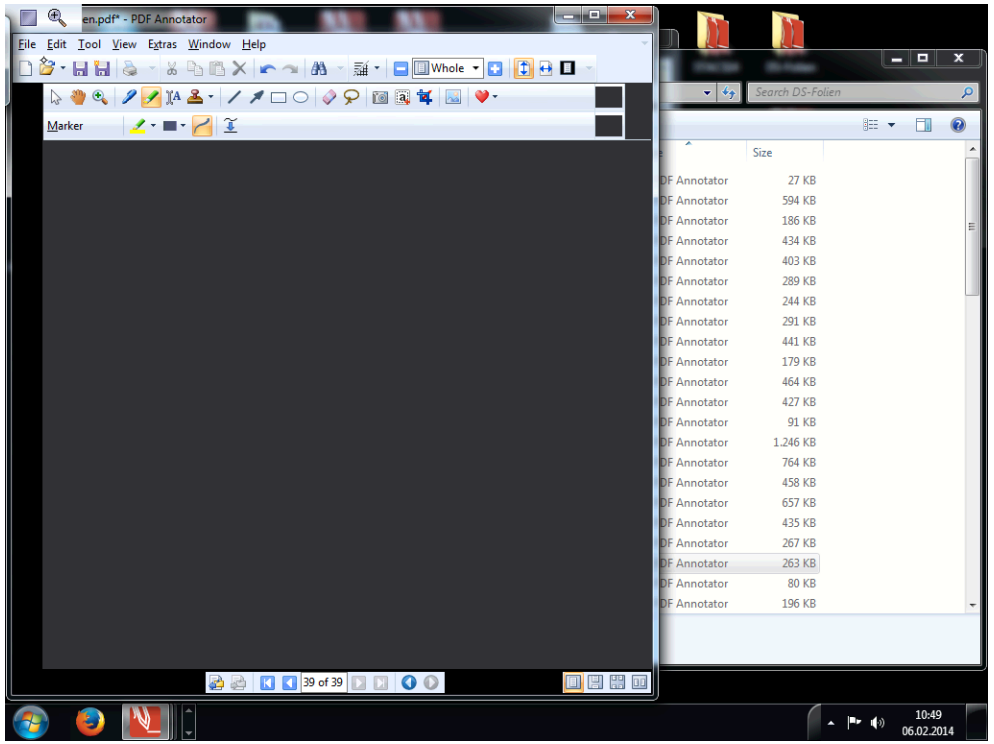
  Sei U_n die Menge aller Permutationen $\{1, \dots, n\} \to \{1, \dots, n\}$.

  Die Symmetrische Gruppe für n Elemente ist die Gruppe $S_n = \langle U_n, \circ \rangle$, wobei „$\circ$“ die Komposition von Abbildungen bezeichnet.

Kapitel V – Algebra; Gruppen

- Für $n = 3$ enthält S_3 sechs verschieden Permutationen:

∘	(1)(2)(3)	(1)(23)	(12)(3)	(13)(2)	(123)	(132)
(1)(2)(3)	(1)(2)(3)	(1)(23)	(12)(3)	(13)(2)	(123)	(123)
(1)(23)	(1(23)	(1)(2)(3)	(132)	(123)	(13)(2)	(12)(3)
(12)(3)						
(13)(2)			…			
(123)						
(132)						



Kapitel V – Algebra; Körper

- Ringe und Körper

  Definition: Eine Algebra $\langle S, \oplus, \odot \rangle$ mit zweistelligen Operatoren $\oplus$ und $\odot$ heißt Ring falls

  (1) $\langle S, \oplus \rangle$ ist eine abelsche Gruppe.

  (2) $\langle S, \odot \rangle$ ist ein Monoid.

  (3) Die Distributivgesetze gelten:

  - $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
  - $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$

Kapitel V – Algebra; Körper

- Ringe und Körper

  Beispiele:

  - $\langle \mathbb{Z}, +, * \rangle$ ist Ring.
  - $\langle \mathbb{Z}_n, +_n, *_n \rangle$ ist Ring für alle $n \geq 1$.
  - $\langle \mathbb{Q}, +, * \rangle$ und $\langle \mathbb{R}, +, * \rangle$ sind Körper.
  - $\langle \mathbb{Z}_3, +_3, *_3 \rangle$ ist Körper.

Kapitel V – Algebra; Körper

- Ringe und Körper

  Definition: Eine Algebra $\langle S, \oplus, \odot \rangle$ mit zweistelligen Operatoren $\oplus$ und $\odot$ heißt Ring falls

  (1) $\langle S, \oplus \rangle$ ist eine abelsche Gruppe.

  (2) $\langle S, \odot \rangle$ ist ein Monoid.

  (3) Die Distributivgesetze gelten:

  - $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
  - $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$

3

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebra; Körper

- Ringe und Körper

  Definition: Eine Algebra $\langle S, \oplus, \odot \rangle$ mit zweisteligen Operatoren $\oplus$ und $\odot$ heißt Körper falls

  (1) $\langle S, \oplus \rangle$ ist eine abelsche Gruppe mit neutralem Element **0**.

  (2) $\langle S \setminus \{\mathbf{0}\}, \odot \rangle$ ist eine abelsche Gruppe.

  (3) Das Linksdistributivgesetz gilt:
  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
  (das Rechtsdistributivgesetz folgt aus den übrigen Eigenschaften)

Kapitel V – Algebra; Körper

- Ringe und Körper

  Beispiele:

  - $\langle \mathbb{Z}, +, * \rangle$ ist Ring.
  - $\langle \mathbb{Z}_n, +_n, *_n \rangle$ ist Ring für alle $n \geq 1$.
  - $\langle \mathbb{Q}, +, * \rangle$ und $\langle \mathbb{R}, +, * \rangle$ sind Körper.
  - $\langle \mathbb{Z}_3, +_3, *_3 \rangle$ ist Körper.

Kapitel V – Algebra; Körper

- Zahlenkörper

  Satz: Für alle $n \geq 2$:

  $\langle \mathbb{Z}_n, +_n, *_n \rangle$ ist ein Körper gdw. n ist eine Primzahl.

  Beweis: Für alle $n \geq 2$ erfüllt $\langle \mathbb{Z}_n, +_n, *_n \rangle$ alle Eigenschaften eines Körpers bis auf die Existenz von multiplikativen Inversen in $\langle \mathbb{Z}_n \setminus \{0\}, *_n \rangle$.

  Diese existieren gdw. n ist eine Primzahl.

Kapitel V – Algebra; Körper

- Zahlenkörper

  Satz: Für alle $n \geq 2$:

  $\langle \mathbb{Z}_n, +_n, *_n \rangle$ ist ein Körper gdw. n ist eine Primzahl.

  Beweis: Für alle $n \geq 2$ erfüllt $\langle \mathbb{Z}_n, +_n, *_n \rangle$ alle Eigenschaften eines Körpers bis auf die Existenz von multiplikativen Inversen in $\langle \mathbb{Z}_n \setminus \{0\}, *_n \rangle$.

  Diese existieren gdw. n ist eine Primzahl.

7

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebra; Körper

- Ringe und Körper

  Definition: Eine Algebra $\langle S, \oplus, \odot \rangle$ mit zweisteligen Operatoren $\oplus$ und $\odot$ heißt Körper falls

  (1) $\langle S, \oplus \rangle$ ist eine abelsche Gruppe mit neutralem Element **0**.

  (2) $\langle S \setminus \{\mathbf{0}\}, \odot \rangle$ ist eine abelsche Gruppe.

  (3) Das Linksdistributivgesetz gilt:

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

  (das Rechtsdistributivgesetz folgt aus den übrigen Eigenschaften)

Kapitel V – Algebra; Körper

- Zahlenkörper

  Satz: Für alle $n \geq 2$:

  $\langle \mathbb{Z}_n, +_n, *_n \rangle$ ist ein Körper gdw. n ist eine Primzahl.

  Beweis: Für alle $n \geq 2$ erfüllt $\langle \mathbb{Z}_n, +_n, *_n \rangle$ alle Eigenschaften eines Körpers bis auf die Existenz von multiplikativen Inversen in $\langle \mathbb{Z}_n \setminus \{0\}, *_n \rangle$.

  Diese existieren gdw. n ist eine Primzahl.

Kapitel V – Algebra; Körper

- Polynomkörper
  - Die Elemente des Körpers sind nicht mehr Zahlen, sondern Polynome.
  - Wir erweitern die Begriffe Summe, Produkt, Division, Rest, Modulo, und Primzahl auf Polynome.
  - Wir führen dann einen zweiten Satz über die Existenz endlicher Körper ein.

Kapitel V – Algebra; Körper

- Polynome

  Definition: Sei $\langle K, +, \cdot \rangle$ ein (kommutativer) Ring. Ein Polynom über K in der Variablen x ist ein Ausdruck der Gestalt.

  $$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$$

  wobei $n \in \mathbb{N}_0$, $a_i \in K$ und $a_n \neq 0$.

  Der Grad des Polynoms ist n und seine Koeffizienten sind $a_0, \ldots, a_n$.

  $K[x]$ bezeichnet die Menge der Polynome über dem Ring K in der Variablen x.

Kapitel V – Algebra; Körper

- Operationen auf Polynomen
  - Seien zwei Polynome

    $$a(x) = a_n x^n + \cdots + a_1 x + a_0$$
    $$b(x) = b_n x^n + \cdots + b_1 x + b_0$$

  - Die Summe $(a + b)(x)$ ist das Polynom

    $$(a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

  - Die Differenz $(a - b)(x)$ ist das Polynom

    $$(a_n - b_n)x^n + \cdots + (a_1 - b_1)x + (a_0 - b_0)$$

    wobei $-b_i$ das inverse Element von b_i bezüglich der Summe darstellt.

Kapitel V – Algebra; Körper

- Operationen auf Polynomen

  Das Produkt zweier Polynome

$$a(x) = a_n x^n + \cdots + a_1 x + a_0$$
$$b(x) = b_m x^m + \cdots + b_1 x + b_0$$

  erhält man durch Ausmultiplizieren und anschließendes Sortieren und Zusammenfassen der Koeffizienten, also

$$(a \cdot b)(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \cdots$$
$$= \sum_{i=0}^{m+n} \sum_{j=0}^{i} a_j b_{i-j} x^i$$

Kapitel V – Algebra; Körper

- Operationen auf Polynomen

  Beispiel

$$2x^4 + x^3 + \quad x + 3 \text{ div } x^2 + x - 1 = 2x^2 - x + 3$$
$$-(2x^4 + 2x^3 - 2x^2)$$
$$-x^3 + 2x^2 + x + 3$$
$$-(-x^3 - x^2 + x)$$
$$3x^2 + 3$$
$$-(3x^2 + 3x - 3)$$
$$-3x + 6$$

Kapitel V – Algebra; Körper

- Operationen auf Polynomen

  Beispiel mit $\mathbb{Z}_6$ als Ring :

  Für $a(x) = x^2 + 3x + 5$ und $b(x) = 4x + 2$ ergibt sich

$$(a \cdot b)(x) = (1 \cdot 4)x^3 + (1 \cdot 2 + 3 \cdot 4)x^2 +$$
$$(3 \cdot 2 + 5 \cdot 4)x + 5 \cdot 2$$
$$= 4x^3 + 2x^2 + 2x + 4.$$

Kapitel V – Algebra; Körper

- Operationen auf Polynomen
  - Seien zwei Polynome

$$a(x) = a_n x^n + \cdots + a_1 x + a_0$$
$$b(x) = b_n x^n + \cdots + b_1 x + b_0$$

  - Die Summe $(a + b)(x)$ ist das Polynom

$$(a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

  - Die Differenz $(a - b)(x)$ ist das Polynom

$$(a_n - b_n)x^n + \cdots + (a_1 - b_1)x + (a_0 - b_0)$$

    wobei $-b_i$ das inverse Element von b_i bezüglich der Summe darstellt.

Kapitel V – Algebra; Körper

- Polynomkörper

  Definition: Ein Polynom $\pi(x) \in K[x]$ mit $\pi(x) \neq 0$ heißt irreduzibel falls für alle $f(x), g(x) \in K[x]$ gilt: wenn $\pi(x) = f(x) \cdot g(x)$, dann $\text{grad}(f) = 0$ oder $\text{grad}(g) = 0$.