

# Entscheidungsverfahren mit Anwendungen in der Softwareverifikation

## **II: Algebraische und logische Grundlagen**

---

Carsten Sinz  
Institut für Theoretische Informatik

29.10.2019

- **Algebraische Grundlagen**

- Algebraische Strukturen: Gruppe, Körper, Ring, ...
- Speziellere Strukturen: euklidischer Ring, ...

- **Logische Grundlagen**

- Aussagenlogik
- Prädikatenlogik erster Stufe

- **Definition (Gruppe):** Eine Gruppe ist ein Paar  $(G, \star)$  bestehend aus einer Menge  $G$  und einer zweistelligen Verknüpfung  $\star : G \times G \rightarrow G$ , wobei für  $(G, \star)$  die folgenden Axiome gelten:
  - Assoziativgesetz:  $\forall a, b, c \in G : (a \star b) \star c = a \star (b \star c)$
  - Neutralement:  $\exists e \in G : \forall a \in G : a \star e = e \star a = a$
  - Inverses Element:  $\forall a \in G : \exists a^{-1} \in G : a \star a^{-1} = a^{-1} \star a = e$
- **Definition:** Falls die Operation  $\star$  kommutativ ist, d.h. wenn
$$\forall a, b \in G : a \star b = b \star a$$
so heißt die Gruppe *kommutativ* oder *abelsch*.
- **Beispiele:**
  - $(\mathbb{Z}, +)$ ,  $(\mathbb{Q} \setminus \{0\}, *)$  sind abelsche Gruppen
  - Die Menge aller invertierbaren  $n \times n$  - Matrizen zusammen mit der Matrixmultiplikation bilden eine (nicht-kommutative Gruppe)

- **Definition (Körper):** Ein Körper (engl. *field*) ist ein Tripel  $(K, +, \cdot)$  bestehend aus einer Menge  $K$  und zwei zweistelligen Verknüpfungen  $+, \cdot : K \times K \rightarrow K$ , wobei die folgenden Bedingungen erfüllt sind:
  1.  $(K, +)$  ist eine abelsche Gruppe (Neutralelement wird mit  $0$  bezeichnet)
  2.  $(K \setminus \{0\}, \cdot)$  ist eine abelsche Gruppe (Neutralelement wird mit  $1$  bezeichnet)
  3. Distributivgesetz:  $\forall a, b, c \in K : a \cdot (b + c) = a \cdot b + a \cdot c$
- **Notation:** Das Inverse von  $a$  bzgl. Addition ( $+$ ) wird mit  $-a$  bezeichnet, das Inverse bzgl. Multiplikation mit  $a^{-1}$ .
- **Beispiele:**
  - $(\mathbb{Q}, +, \cdot), (\mathbb{C}, +, \cdot)$  sind Körper.
  - $(\mathbb{Z}/p\mathbb{Z})$  für eine Primzahl  $p$  sind endliche Körper

- **Definition (Ring):** Ein Ring ist ein Tripel  $(R, +, \cdot)$  bestehend aus einer Menge  $K$  und zwei zweistelligen Verknüpfungen  $+, \cdot : R \times R \rightarrow R$ , wobei die folgenden Bedingungen erfüllt sind:

1.  $(R, +)$  ist eine abelsche Gruppe (Neutralelement wird mit 0 bezeichnet),
2.  $(R, \cdot)$  ist eine Halbgruppe (d.h.  $\cdot$  ist assoziativ),
3. Die Distributivgesetze

$$\forall a, b, c \in K : a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und}$$

$$\forall a, b, c \in K : (a + b) \cdot c = a \cdot c + b \cdot c$$

gelten.

- **Definition:** Ein Ring heißt *unitär* oder *Ring mit Eins*, falls  $(R, \cdot)$  ein Monoid ist, d.h., falls es ein (beidseitiges) Neutralelement 1 in  $R$  gibt.

- **Beispiele:**

- Jeder Körper ist auch ein Ring
- $\mathbb{Z}$ , Polynome

- **Definition (Ideal):** Zu einem Ring  $(R, +, \cdot)$  heißt eine Teilmenge  $I$  von  $R$  Linksideal bzw. Rechtsideal, wenn gilt:

1.  $I$  ist eine Untergruppe von  $(R, +)$

2. Abschluss:  $\forall a \in I : \forall x \in R : x \cdot a \in I$  (Linksideal) oder  
 $\forall a \in I : \forall x \in R : a \cdot x \in I$  (Rechtsideal)

Ist  $I$  sowohl Links- als auch Rechtsideal, so heißt es *Ideal*.

- **Beispiel:**

- Die Menge der geraden Zahlen,  $2\mathbb{Z}$ , ist ein Ideal im Ring  $\mathbb{Z}$  der ganzen Zahlen

- **Eigenschaften:**

- Enthält ein Ideal zu einem Ring  $R$  die 1, so umfasst es ganz  $R$ .

- **Definition (Polynomring):** Ist  $R$  ein kommutativer Ring mit  $1$ , so kann der Polynomring  $R[X]$  gebildet werden, der aus Polynomen mit Koeffizienten aus  $R$  und der Variablen  $X$  besteht mit der üblichen Addition und Multiplikation für Polynome.
- **Definition (Faktoring):** Ist  $(R, +, \cdot)$  ein Ring und  $I$  ein Ideal von  $R$ , denn bildet die Menge  $R/I = \{a + I \mid a \in R\}$  der Äquivalenzklassen modulo  $I$  mit folgenden Verknüpfungen einen Ring („Faktoring  $R$  modulo  $I$ “, „Restklassenring“, „Quotientenring“):
$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I) \cdot (b + I) = (a \cdot b) + I$$
- **Beispiele:**
  - $\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$
  - Sei  $f \in R[X]$  ein Polynom, und  $(f) := R[X] \cdot f$  die Menge aller Polynom-Vielfachen von  $f$ . Dann ist  $(f)$  ein Ideal und  $R[X]/(f) = \{g + (f) \mid g \in R[X]\}$  ist der Faktoring  $R[X]$  modulo  $f$ . Bsp.:  $\mathbb{R}[X]/(X^2 + 1)$

- **Definition (Nullteiler):** Ein Element  $a \in R$  eines kommutativen Rings  $R$  heißt *Nullteiler*, falls es ein  $b \neq 0$  gibt mit  $a \cdot b = 0$ .
- **Definition (Integritätsbereich):** Ein vom Nullring (d.h.  $R = \{0\}$ ) verschiedener nullteilerfreier kommutativer Ring mit 1 heißt *Integritätsbereich* oder *Integritätsring*.
- **Beispiel:**
  - $\mathbb{Z}, \mathbb{Z}[X]$  (allgemeiner: Polynome mit Koeffizienten aus einem Integritätsber.)
  - $\mathbb{Z}/4\mathbb{Z}$  ist kein Integritätsbereich, da nicht nullteilerfrei
- **Eigenschaften:**
  - Auf einem Integritätsbereich kann man Teilbarkeit definieren
    - $a$  teilt  $b$  (in Zeichen:  $a|b$ ), wenn es ein  $x \in R$  gibt mit  $a \cdot x = b$

- **Definition (Euklidischer Ring):** Ein Integritätsring heißt *euklidischer Ring*, falls es eine Bewertungsfunktion  $g : R \setminus \{0\} \rightarrow \mathbb{N}$  gibt mit:
  - Für alle  $x, y \in R$  mit  $y \neq 0$  gibt es Elemente  $q, r \in R$  mit  $x = q \cdot y + r$ , wobei entweder  $r = 0$  oder  $g(r) < g(y)$  ist (Division mit Rest)
  - Für alle  $x, y \in R \setminus \{0\}$  gilt:  $g(x \cdot y) \geq g(x)$
- **Beispiele:**
  - $\mathbb{Z}$  mit  $g(x) = |x|$
  - $K[X]$ , wobei  $g(p) = \text{grad } p$
- **Bemerkung:**
  - Die Definition lässt sich erweitern auf Ringe mit Nullteilern.

- **Syntax:**

- Sei  $V = \{ x, y, z, \dots \}$  eine Menge von Aussagevariablen
- Die Menge der aussagenlogischen Formeln  $F$  ist definiert als kleinste Menge, für die gilt:
  - $V \subseteq F$
  - $\perp \in F$  ( $\perp$  steht für „falsch“)
  - Ist  $f, g \in F$ , so auch  $(f \vee g)$ ,  $(f \wedge g)$  und  $\neg f$

- **Semantik:**

- Eine *Variablenbelegung* ist eine Funktion  $\beta: V \longrightarrow \{ 0, 1 \}$ , die jeder Aussagenvariable einen Wahrheitswert (0: falsch, 1: wahr) zuweist.
- Gegeben eine Variablenbelegung  $\beta$ , kann eine Formel  $f$  *evaluiert* werden, mittels:  
$$\beta(\perp) = 0, \quad \beta(\neg f) = 1 - \beta(f), \quad \beta(f \vee g) = \max(\beta(f), \beta(g)), \quad \beta(f \wedge g) = \min(\beta(f), \beta(g))$$

- **Definitionen:**

- Eine (aussagenlogische) Formel  $f$  heißt *erfüllbar*, wenn es eine Variablenbelegung  $\beta$  gibt mit  $\beta(f)=1$ . Ansonsten heißt  $f$  *unerfüllbar*.
- Eine Formel heißt allgemeingültig (oder gültig), wenn für alle Variablenbelegungen  $\beta$  gilt  $\beta(f)=1$ .

- **Anmerkung:**

- Erfüllbarkeit und Allgemeingültigkeit sind duale Begriffe

- Seien  $V$ ,  $F$ ,  $R$  disjunkte Mengen.
  - $V$ : Menge der (Objekt-)Variablen
  - $F$ : Menge der Funktionssymbole (jeweils mit Stelligkeit  $a(f) \in \mathbb{N}$ )
  - $R$ : Menge der Relationssymbole (jeweils mit Stelligkeit  $a(r) \in \mathbb{N}$ )
- **Definition (Term):** Die Menge  $T = T(V, F)$  der Terme über  $V$  und  $F$  ist definiert als kleinste Menge, so dass:
  - $V \subseteq T$
  - Falls  $a(f) = n$  und  $t_1, \dots, t_n \in T$ , so auch  $f(t_1, \dots, t_n)$

- Seien  $V$ ,  $F$ ,  $R$  disjunkte Mengen.
  - $V$ : Menge der (Objekt-)Variablen
  - $F$ : Menge der Funktionssymbole (jeweils mit Stelligkeit  $s(f) \in \mathbb{N}$ )
  - $R$ : Menge der Relationssymbole (jeweils mit Stelligkeit  $s(r) \in \mathbb{N}$ )
- **Definition (PL1-Formel)**: Die Menge  $P = P(V, F, R)$  der Formeln der Prädikatenlogik erster Stufe (PL1-Formeln) über  $V$ ,  $F$  und  $R$  ist definiert als die kleinste Menge, so dass:
  - $\perp \in P$
  - Falls  $r \in R$  mit  $s(r) = n$ , und  $t_1, \dots, t_n \in T(V, F)$ , so ist  $r(t_1, \dots, t_n) \in P$
  - Falls  $f, g \in P$ , so auch  $(f \vee g)$ ,  $(f \wedge g)$  und  $\neg f$
  - Falls  $x \in V$  und  $f \in P$ , so auch  $\exists x.f$  und  $\forall x.f$

- **Definition ((F, R)-Struktur):** Sei  $F$  eine Menge von Funktionssymbolen und  $R$  eine Menge von Relationssymbolen. Eine  $(F, R)$ -Struktur ist ein Tupel  $\mathbf{A} = (A, a)$ , wobei
  - $A$  eine nichtleere Menge, das *Universum* von  $\mathbf{A}$  ist.
  - $a$  eine Funktion, die jedem  $f \in F$  eine  $s(f)$ -stellige Funktion  $a(f) : A^n \longrightarrow A$  und jedem  $r \in R$  eine  $s(r)$ -stellige Relation  $a(r) = A^n$  zuordnet.
- **Definition (Variablenbelegung):** Sei  $V$  eine Variablenmenge und  $\mathbf{A} = (A, a)$  eine  $(F, R)$ -Struktur. Eine Variablenbelegung (für  $V$  in  $A$ ) ist eine Abbildung  $\beta: V \longrightarrow A$ , die jeder Variable ein Element des Universums zuweist.
- **Definition (Interpretation):** Eine Interpretation  $I$  (zu gegebenen  $V, F$  und  $R$ ) ist ein Tupel  $(\mathbf{A}, \beta)$  bestehend aus einer  $(F, R)$ -Struktur und einer Variablenbelegung  $\beta$  für  $V$  in  $A$ .

- **Definition (Interpretation eines Terms):** Sei  $I = (\mathbf{A}, \beta)$  eine Interpretation. Für einen Term  $t$  definier wir dessen Interpretation  $I(t)$  rekursiv durch:
  - $I(t) = \beta(t)$ , falls  $t \in V$ ,
  - $I(f(t_1, \dots, t_n)) = a(f)(I(t_1), \dots, I(t_n))$
- **Definition (Erfüllbarkeitsrelation):** Sei  $I = (\mathbf{A}, \beta)$  eine Interpretation. Wir definieren die Erfüllbarkeitsrelation  $I \models f$  für Formeln  $f$  wie folgt:
  - $I \not\models \perp$
  - $I \models r(t_1, \dots, t_n)$       gdw.       $a(r)(I(t_1), \dots, I(t_n))$
  - $I \models (f \vee g)$       gdw.       $I \models f$  oder  $I \models g$
  - $I \models (f \wedge g)$       gdw.       $I \models f$  und  $I \models g$
  - $I \models \neg f$       gdw.       $I \not\models f$
  - $I \models \forall x.f$       gdw.       $I[x/e] \models f$  für alle  $e \in A$
  - $I \models \exists x.f$       gdw.      es gibt ein  $e \in A$  mit  $I[x/e] \models f$

- K. O. Geddes, S.R. Czapor, G. Laban (1992):  
Algorithms for Computer Algebra,  
Kluwer, ISBN 0-7923-9259-0
- Melvin Fitting (2013):  
First-Order Logic and Automated Theorem Proving (2nd Ed.),  
Springer, ISBN 1-4612-7515-6