FAKULTÄT
FÜR !NFORMATIK

Faculty of Informatics

Formal Semantics of Programming Languages

Florian Zuleger

SS 2014

Group Axioms – informal

(G, $\cdot$, e) is a group, if

- $\cdot$ is a binary relation on G,
- e is a special element of G called the **neutral element**,
- $x \cdot e = x$ and $e \cdot x = x$ for all $x \in G$,
- for all $x \in G$ there is a $y \in G$ such that $x \cdot y = e$ and $y \cdot x = e$ called the **inverse element**, and
- $\cdot$ is associative, i.e., $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x,y,z \in G$.

Group Axioms – in First Order Logic

Signature ($\cdot$, e),

- where the function $\cdot$ has arity 2,
- and the function e has arity 0 (i.e., a constant).

Axioms:

G1: $\forall$ x. x $\cdot$ e = x $\wedge$ e $\cdot$ x = x

G2: $\forall$ x. $\exists$ y. x $\cdot$ y = e $\wedge$ y $\cdot$ x = e

G3: $\forall$ x. $\forall$ y. $\forall$ z. x $\cdot$ (y $\cdot$ z) = (x $\cdot$ y) $\cdot$ z

All **models** that simultaneously satisfy G1, G2 and G3 are called **groups**.

Examples

$(\mathbb{Z},+,0)$

$(\mathbb{Z},\cdot,1)$?

$(\mathbb{Q},\cdot,1)$

$(\mathbb{R},\cdot,1)$

$(\mathbb{Z}/n\mathbb{Z}, +,0)$ (the so-called cyclic group)

(C unsigned integers,+,0)

$(\mathrm{Sym}_n, \circ, \mathrm{id})$ (the permutations of n elements)

Weaker Group Axioms

Signature ($\cdot$, e),

- where $\cdot$ has arity 2,
- and e has arity 0.

Axioms:

W1: $\forall$ x. x $\cdot$ e = x

W2: $\forall$ x. $\exists$ y. x $\cdot$ y = e

G3: $\forall$ x. $\forall$ y. $\forall$ z. x $\cdot$ (y $\cdot$ z) = (x $\cdot$ y) $\cdot$ z

However, W1, W2 and G3 imply G1 and G2 (see next slides)! (Recall the definition of implication: all models of W1, W2 and G3 satisfy G1 and G2)

W1, W2 and G3 imply G2 - Informal

Let G be some group.

Let x be some element of G.

By W2 there is a y such that xy = e.

By W1 we have (y(xy))x = (ye)x = yx (*).

By W2 there is a z such that (xy)z = e (#).

Multiply z from the right on both sides of (*):

((y(xy))x)z = (yx)z.

From (#) and associativity (G3) we get: (yx)e = e.

From W2 we get yx = e.

Because x was chosen arbitrary this holds for all elements of G.

W1, G2 and G3 imply G1 - Informal

Let G be some group.

Let x be some element of G.

By G2 there is a y such that $xy = e$ and $yx=e$.

Thus we have $ex = (xy)x = x(yx) = xe$ using associativity (G3).

By W1 we have $ex = xe = x$.

Because x was chosen arbitrary this holds for all elements of G.

Questions

- Is this proof correct, i.e., is every model of W1, W2 and G3 also a model of G1, G2 and G3?
- How can we verify the correctness of the proof?
- Can the proof be automated?
- Can proofs always be automated (i.e., are valid sentences decidable)?

$\rightarrow$ We define a proof calculus for FOL and prove its soundness and completeness.

$\rightarrow$ We establish the undecidability of FOL.

Refutation Calculus

$$\text{N1}\ \frac{\models \neg F}{\not\models F} \qquad \text{N2}\ \frac{\not\models \neg F}{\models F} \qquad \text{F1}\ \frac{\models \forall x.\, F(x)}{\models F(t)} \qquad \text{F2}\ \frac{\not\models \forall x.\, F(x)}{\not\models F(c)}$$

c is a fresh constant

$$\text{A1}\ \frac{\models F \wedge G}{\begin{array}{l}\models F\\ \models G\end{array}} \qquad \text{A2}\ \frac{\not\models F \wedge G}{\not\models F \mid \not\models G} \qquad \text{E2}\ \frac{\not\models \exists x.\, F(x)}{\not\models F(t)} \qquad \text{E1}\ \frac{\models \exists x.\, F(x)}{\models F(c)}$$

c is a fresh constant

$$\text{O1}\ \frac{\not\models F \vee G}{\begin{array}{l}\not\models F\\ \not\models G\end{array}} \qquad \text{O2}\ \frac{\models F \vee G}{\models F \mid \models G}$$

$$\text{Id}\ \frac{}{\models t = t} \qquad \text{S1}\ \frac{\models F(t) \quad \models s = t}{\models F(s)}$$

$$\text{S2}\ \frac{\not\models F(t) \quad \models s = t}{\not\models F(s)}$$

$$\text{C1}\ \frac{\begin{array}{l}\models P(c_1,c_2,\ldots,c_n)\\ \not\models P(c_1,c_2,\ldots,c_n)\end{array}}{\bot}$$

<u>Goal:</u> Proof for a valid sentence F

<u>Idea:</u> Assume $\not\models F$ and find a contradiction in every branch of the proof

Examples

- $F \vee \neg F$
- $(F \vee \neg F) \wedge (G \vee \neg G)$
- $\forall x.\ F(x) \vee \exists x.\ \neg F(x)$
- $F(a) \wedge \exists x.\ \neg F(x)$?
- W1, G2 and G3 imply G1, i.e.,

  $W1 \wedge G2 \wedge G3 \rightarrow G1$

Example Proof

(1) $\not\models F \vee \neg F$

(2) $\not\models F$ (from (1) by O2)

(3) $\not\models \neg F$ (from (1) by O2)

(4) $\models F$ (from (3) by N2)

(5) $\perp$ (from (2) and (4) by C)

Example Proof

(1) $\not\models (F \vee \neg F) \wedge (G \vee \neg G)$

(2) $\not\models F \vee \neg F$ (from (1) by A2)

(3) $\not\models F$ (from (1) by O2)

(4) $\not\models \neg F$ (from (1) by O2)

(5) $\models F$ (from (3) by N2)

(6) $\perp$ (from (2) and (4) by C)

(7) $\not\models G \vee \neg G$ (from (1) by A2)

(8) $\not\models G$ (from (7) by O2)

(9) $\not\models \neg G$ (from (7) by O2)

(10) $\models G$ (from (9) by N2)

(11) $\perp$ (from (8) and (10) by C)

Example Proof

(1) $\not\models \forall x.\ F(x) \vee \exists x.\ \neg F(x)$

(2) $\not\models \forall x.\ F(x)$ (from (1) by O2)

(3) $\not\models \exists x.\ \neg F(x)$ (from (1) by O2)

(4) $\not\models F(c)$ (from (2) by A2)

(5) $\not\models \neg\ F(c)$ (from (3) by E2)

(6) $\models F(c)$ (from (5) by N2)

(7) $\perp$ (from (4) and (6) by C)

Example Proof – Wrong!

(1) $\not\models F(a) \vee \forall x. \neg F(x)$

(2) $\not\models F(a)$ (from (1) by O2)

(3) $\not\models \forall x. \neg F(x)$ (from (1) by O2)

(4) $\not\models \neg F(a)$ (from (3) by F2)

(5) $\models F(a)$ (from (4) by N2)

(6) $\bot$ (from (2) and (5) by C)

a is **not** a fresh constant!

Note that $F(a) \vee \forall x. \neg F(x)$ is not valid!

Example Proof – Correct!

(1) $\not\models F(a) \vee \forall x. \neg F(x)$

(2) $\not\models F(a)$ (from (1) by O2)

(3) $\not\models \forall x. \neg F(x)$ (from (1) by O2)

(4) $\not\models \neg F(b)$ (from (3) by F2)

(5) $\models F(b)$ (from (4) by N2)

b is a fresh constant!

No contradiction can be inferred!

No further rule is applicable!

(M = (D,I) with D = {A,B}, a^I = A, b^I = B, F^I = {B} is a model that falsifies $F(a) \vee \forall x. \neg F(x)$)

W1, G2 and G3 imply G1 - Informal

Let G be some group.

Let x be some element of G.

By G2 there is a y such that $xy = e$ and $yx=e$.

Thus we have $ex = (xy)x = x(yx) = xe$ using associativity (G3).

By W1 we have $ex = xe = x$.

Because x was chosen arbitrary this holds for all elements of G.

Group Axioms – in First Order Logic

Signature ($\cdot$, e),

- where the function $\cdot$ has arity 2,
- and the function e has arity 0 (i.e., a constant).

Axioms:

G1: $\forall$ x. x $\cdot$ e = x $\wedge$ e $\cdot$ x = x

G2: $\forall$ x. $\exists$ y. x $\cdot$ y = e $\wedge$ y $\cdot$ x = e

G3: $\forall$ x. $\forall$ y. $\forall$ z. x $\cdot$ (y $\cdot$ z) = (x $\cdot$ y) $\cdot$ z

All **models** that simultaneously satisfy G1, G2 and G3 are called **groups**.

W1, G2 and G3 imply G1

(1) $\not\models (W1 \wedge G2 \wedge G3) \rightarrow G1$

(2) $\not\models \neg (W1 \wedge G2 \wedge G3) \vee G1$ (Rewrite of $\rightarrow$)

(3) $\not\models \neg (W1 \wedge G2 \wedge G3)$ (from (2) by O2)

(4) $\not\models G1$ (from (2) by O2)

(5) $\models W1 \wedge G2 \wedge G3$ (from (3) by N2)

(6) $\models W1$ (from (5) by A1)

(7) $\models G2 \wedge G3$ (from (5) by A1)

(8) $\models G2$ (from (7) by A1)

(9) $\models G3$ (from (7) by A1)

(10) $\not\models c \cdot e = c \wedge e \cdot c = c$ (from (4) by F2)

(11) $\models \exists y.\ c \cdot y = e \wedge y \cdot c = e$ (from (8) by F1)

(12) $\models c \cdot d = e \wedge d \cdot c = e$ (from (10) by E1)

(13) $\models c \cdot d = e$ (from (11) by A1)

(14) $\models d \cdot c = e$ (from (11) by A1)

W1, G2 and G3 imply G1

(15) $\models c \cdot e = c$ (from (6) by F1)

(16) $\models c \cdot (d \cdot c) = c$ (from (15) and (16) by S1)

(17) $\models \forall y.\, \forall z.\, c \cdot (y \cdot z) = (c \cdot y) \cdot z$ (from (10) by F1)

(18) $\models \forall z.\, c \cdot (d \cdot z) = (c \cdot d) \cdot z$ (from (17) by F1)

(19) $\models c \cdot (d \cdot c) = (c \cdot d) \cdot c$ (from (18) by F1)

(20) $\models (c \cdot d) \cdot c = c$ (from (16) and (19) by S1)

(21) $\models e \cdot c = c$ (from (13) and (20) by S1)

(22) $\not\models c \cdot e = c$ (from (10) by A2)

(23) $\bot$ (from (15) and (22) by C)

(24) $\not\models e \cdot c = c$ (from (10) by A2)

(25) $\bot$ (from (21) and (24) by C)

Refutation Calculus - Simplified

$$\text{N1}\ \frac{\models \neg F}{\not\models F} \qquad \text{N2}\ \frac{\not\models \neg F}{\models F} \qquad \text{F1}\ \frac{\models \forall x.\, F(x)}{\models F(t)} \qquad \text{F2}\ \frac{\not\models \forall x.\, F(x)}{\not\models F(c)}$$

c is a fresh constant

$$\text{A1}\ \frac{\models F \wedge G}{\begin{array}{l}\models F\\ \models G\end{array}} \qquad \text{A2}\ \frac{\not\models F \wedge G1}{\not\models F \mid \not\models G}$$

$$\text{C1}\ \frac{\models P(c_1,c_2,\ldots,c_n) \qquad \not\models P(c_1,c_2,\ldots,c_n)}{\bot}$$

<u>Goal:</u> Proof for a valid sentence F

<u>Idea:</u> Assume $\not\models F$ and find a contradiction in every branch of the proof

Simplification

- $\vee$ and $\exists$ can be expressed by $\neg$, $\wedge$ and $\forall$
- We eliminate function symbols: for every occurrence of f in a predicate $L(f(t_1,\ldots t,_n))$ in a formula F we replace this predicate by
  $\exists x.\ P_f(t_1,\ldots t,_n,x) \wedge L(x)$
- For the resulting formula G we add functionality axioms $\wedge_f I_f \rightarrow G$, where I_f denotes the formula $\forall x_1, \ldots, x_n \exists y.\ P_f(x_1,\ldots,x_n,y) \wedge \forall z.\ P_f(x_1,\ldots,x_n,z) \rightarrow y=z$

FOL without Equality

We want to consider FOL without equality.

Thankfully we can describe equality by the following axioms (up to equivalence classes):

Reflexivity (R): $\forall x.\ x = x$

Symmetry (S): $\forall x,y.\ x = y \rightarrow y = x$

Transitivity (T): $\forall x,y,z.\ x = y \wedge y = z \rightarrow x = z$

For every predicate P we define a consistency axiom E_P by $\forall x_1,\ldots,x_n,y_1,\ldots,y_n.\ (x_1=y_1 \wedge \ldots \wedge x_n=y_n) \rightarrow (P(x_1,\ldots,x_n) \leftrightarrow P(y_1,\ldots,y_n))$.

For an FOL formulae F with equality we construct the formula $\wedge_P E_P \wedge R \wedge S \wedge T \rightarrow F$ in FOL without equality.

Terminology

- Note that the proof has the shape of a **tree**.
- We call a line in the proof tree a **branch**.
- We call a branch that contains a contradiction **closed** and a branch without a contradiction **open**.

Proof Construction Algorithm

First line in the proof tree is $\not\models F$.

For every line in the proof exactly one rule can be applied!

We apply this rule once for every line in an open branch of the proof (except for $\models \forall x.\ F(x)$).

We append the results at the end of every open branch to which the line belongs.

The application of rules is fair: for every line a rule is eventually applied and for $\models \forall x.\ F(x)$ the rule is infinitely often applied.

Let c_1, c_2, … be an enumerable sequence of constant symbols that includes all constant symbols from F.

We apply the rule for $\models \forall x.\ F(x)$ for all constants c_1, c_2, … in that order and the rule for $\not\models \forall x.\ F(x)$ with the smallest constant not in the proof.

Either no rule can be applied at some point of time or the algorithm continues forever.

Soundness

Thm

If all branches are closed, F is a valid.

Proof (by contradiction)

Let M be a model for which F does not hold, i.e., M$\not\models$ F.

We show for every rule using the definition: if the premise of the rule holds for M, then the conclusion also holds for M.

For every branch in the proof we extend M according to the additional constants that appear in the proof.

Every branch is closed, i.e., contains a contradiction.

Thus for every branch we know that M cannot be a model of this branch. Contradiction.

Structural Induction

Consider some inductively defined structure given by **axioms** and **constructors**, e.g.,

Tree ::= Leaf | Branch(Tree,Tree).

To prove a property P(T) for every tree T:

- Base case (T = Leaf):
  - prove P(Leaf) is true using known facts
- Induction case (T = Branch(T_1,T_2)):
  - assume the **inductive hypothesis**: P(T_1) and P(T_2) are true
  - prove P(T) is true using known facts and the inductive hypothesis

Example

leaves(Leaf) = 1

leaves(Branch(T_1,T_2)) = leaves(T_1) + leaves(T_2)

branches(Leaf) = 0

branches(Branch(T_1,T_2)) = branches (T_1) + branches (T_2) + 1

leaves(T) = branches(T) + 1 for every Tree T.

Completeness

Thm

If at least one branch is open, F is not valid.

Proof

We choose one (possibly infinite) branch B of the proof tree.

We define a model M as follows:

We set M = {C_1, C_2, … } and we define the interpretation of c_i to be C_i and define M $\models$ P(C_1,C_2,…,C_n) iff P(c_1,c_2,…,c_n) appears on B.

We show by structural induction for every formula G that if G appears on B with $\not\models$ G or $\models$ G, we have M$\not\models$ G or M $\models$ G.

Induction start: By definition of M this holds for all atoms.

Induction step: For G there is exactly one rule applicable, and this rule is applied by the algorithm. The conclusions also appear on B and are structurally smaller so we can apply the induction hypothesis. Using the semantics of FOL we can compose these results to show M$\not\models$ G resp. M $\not\models$ G.

Because $\models$ F appears on B this establishes M $\models$ F .

Further Results

Compactness Theorem

A countable set of first-order formulae S is simultaneously satisfiable iff the conjunction of every finite subset of S is satisfiable.

Proof

Let F_1, F_2, … be an enumeration of S. We apply the above procedure and try to simultaneously prove the validity of every $\neg F_i$, i.e., we construct one joint proof tree and advance every proof of $\neg F_i$ in a fair way. Since each finite subset of S is satisfiable at least one branch will stay open. The resulting model will simultaneously satisfy all F_i.

Corollaries

Löwenheim-Skolem Theorem

Every simultaneously satisfiable countable set of FOL sentences has a countable model.

Semi-Decidability of FOL

The above described algorithm provides a semi-decision procedure for FOL (i.e., it will find a proof for all valid FOL sentences).

Undecidability of FOL

Thm

The language of valid FOL sentences is undecidable.

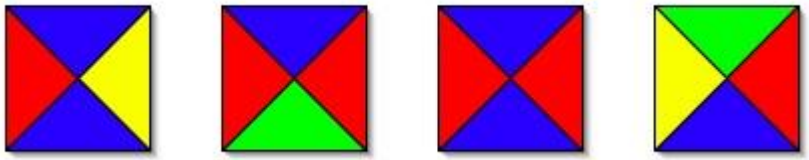
Proof Idea

By reduction from the Halting Problem:

There is an FOL sentence ϕ_M encoding the run (i.e., the sequence of configurations) of a given Turing machine M on an empty input. ϕ_M is valid iff M terminates.

The Tiling Problem (en.wikipedia.org/wiki/Wang_tile)

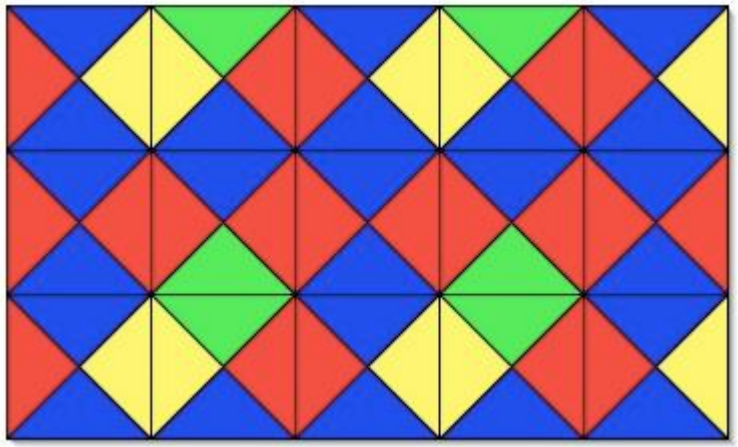
Given a finite set of tiles



is there a tiling of the upper right quadrant such that all colors match (tiles may not be rotated)?

For example,

...



...

The Tiling Problem is known to be undecidable!

Reduction of the Tiling Problem to FOL

Exercise:

- Formal Definition of the Tiling Problem
- Construction of a corresponding FOL formula
- Proof of Reduction: There is a tiling of the upper right quadrant iff the corresponding FOL formula is valid.

Entrance Test (30min)

- Prove implications, equivalences using the semantics of FOL, give counterexamples (i.e., provide models) in case the stated implications, equivalences do not hold
- Use the refutation calculus to prove valid sentences
- Perform proofs by structural induction
- Model problems formally in FOL (e.g., encoding of bit-vector operations in propositional logic, reducing the Tiling Problem to FOL)