Theorem Provers

NatLog Meeting 09/15/2022

Brief Introduction of Theorem Provers, Formal Verification, Category Theory and SAT/SMT solvers.

Sushma Akoju

Theorem Provers : A brief introduction of TPs, Formal Verification, Category Theory and SAT/SMT solvers.

Contents

Topics

Background

https://github.com/yale-lily/folio

https://raw.githubusercontent.com/Yale-LILY/FOLIO/main/data/v0.0/folio-train.jsonl

{"story_id": 8, "example_id": 20, "conclusion": "Miroslav Venhoda loved music.", "premises": ["Miroslav Venhoda was a Czech choral conductor who specialized in the performance of Renaissance and Baroque music.", "Any choral conductor is a musician.", "Some musicians love music.", "Miroslav Venhoda published a book in 1946 called Method of Studying Gregorian Chant."], "premises-FOL": ["Czech(miroslav) ∧ ChoralConductor(miroslav) ∧ Specialize(miroslav, renaissance) ∧ Specialize(miroslav, baroque)", "∀x (ChoralConductor(x) → Musician(x))", "∃x (Musician(x) → Love(x, music))", "Book(methodOfStudyingGregorianChant) ∧ Author(miroslav, methodOfStudyingGregorianChant) ∧ Publish(methodOfStudyingGregorianChant, year1946)"], "label": "Unknown", "source": "wiki"}

Theorem Prover and the Automation

Topics

Theorem Proving Systems

Conjectures and Theories from 1600s

The Kepler Conjecture from 1600s

proven in 1998.

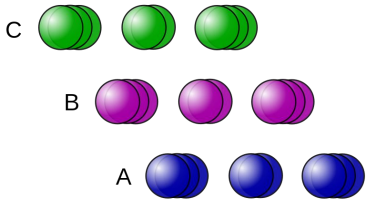
It was noted to be correct only 99%

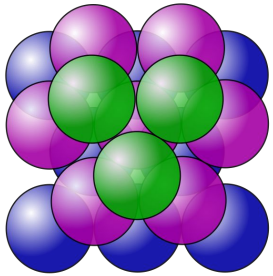
of the time. The need to prove “Theories”

and formally verify in an Automated setting,

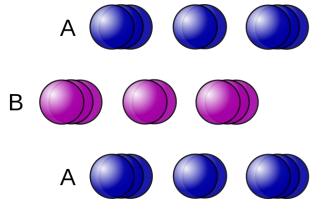
By following satisfiability theory

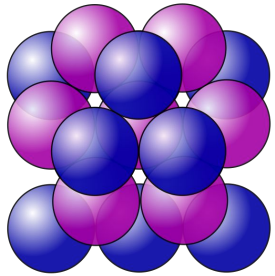
mathematically.





face-centered cubic (fcc)
(also called cubic close packed (ccp))
three repeating layers ABCABC....





hexagonal close-packed (hcp)
two repeating layers ABABAB...

Generalized approach for Theorem Proving (TP)

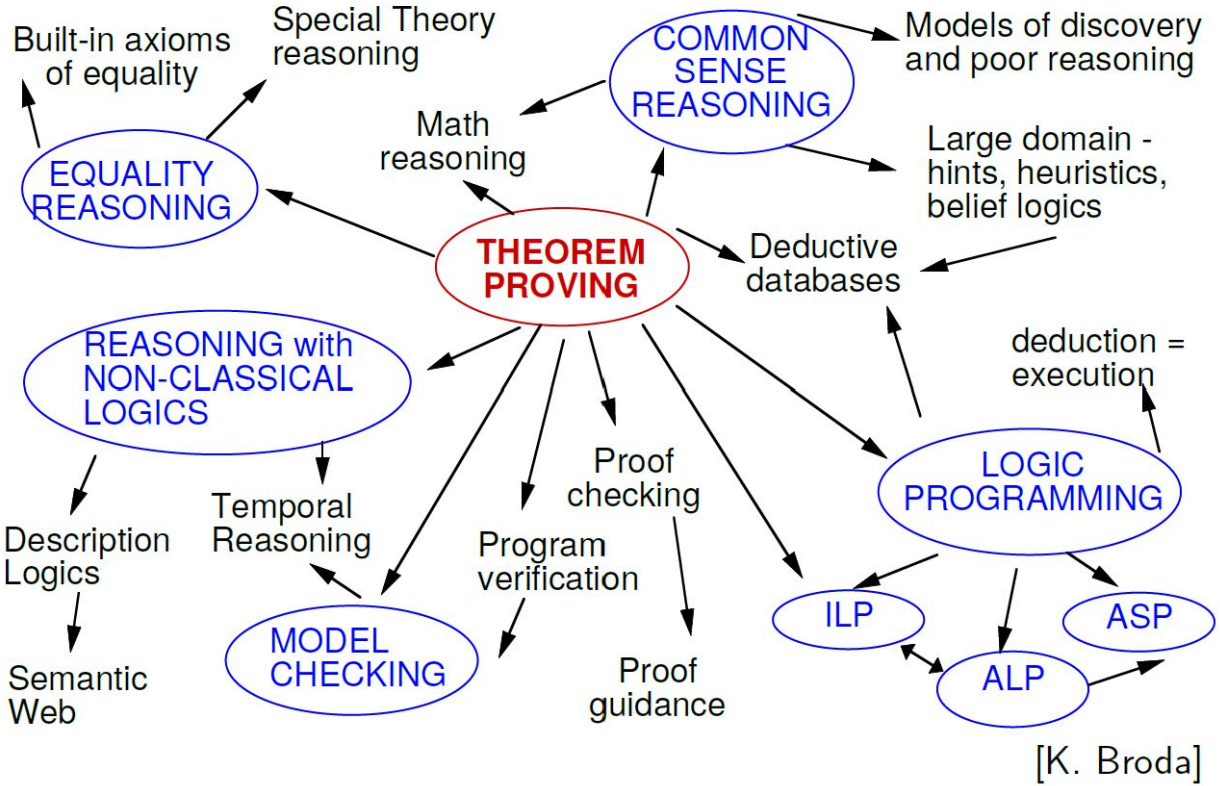
Generalized approach towards Theorem Proving:

1. Formalize the proof using Proof Assistants
2. Implement the computer code in the system
3. Prove the code correct
4. Run the programs inside the Proof Assistant

Example: Compilers

Reference: http://cl-informatik.uibk.ac.at/teaching/ss20/atp2/content.php

Spread of Theorem Provers



The advent of Higher Order Logic (HOL)

1994 - Intel Pentium P5 introduced FPU unit

Birth of Higher Order Logic

Processors were formally verified.

Reference: https://plato.stanford.edu/ and http://cl-informatik.uibk.ac.at/teaching/ss20/atp2/content.php

Example description for this presentation

- Smoking causes cancer
- We need to stop people from smoking
- It's hard to do that since people are influenced by friends
- If friends keep smoking, they are likely to continue smoking

Peer influence doubles smoking risk for adolescents

Teens from collectivistic cultures also more swayed by peers than those in individualistic cultures

Date: August 21, 2017

Source: University of Pennsylvania

Summary: Having friends who smoke doubles the risk that youth ages 10 to 19 will pick up the habit, finds new meta-analysis of 75 longitudinal teen smoking studies. This influence is more powerful in collectivistic cultures than in individualistic ones.

https://www.sciencedaily.com/releases/2017/08/170821102718.htm

Natural Language Beliefs and Logic Statements

- Let us say, we have following beliefs from previous slide:
  - Smoking causes cancer
  - Friends have similar habits
  - Let Alice and Bob be two friends
  - Alice Smokes and has Cancer
  - Alice has Smoking habit
  - Bob has Smoking habit
  - Can Bob get Cancer?
- Should be formally verifiable and expandable enough to prove over various values, edge cases.

Why are Proofs and Provers relevant?

Proofs formalized as objects in their own right.

Offers constructive and syntactic approach towards studying properties of logic

- Consistency
- Decidability
- Interpolation

Helps towards automated reasoning.

Reference: http://nlab-pages.s3.us-east-2.amazonaws.com/nlab

Interpolation

First Order Logic satisfies Interpolation.

I.e. Semantic Entailment relation satisfies Craig Interpolation Theorem.

Craig's INTERPOLATION THEOREM, Let S and T be sentences such that S implies T. Then there exists a sentence M such that S implies M and M implies T, and that a relation symbol has positive occurrences in M if and only if the same exists in S & T and holds for negative occurrences.

Lemma If there is a resolution refutation of size n for a formula A ^ B, there is an interpolant of circuit size 3n that is computable in time n.

Reference: http://nlab-pages.s3.us-east-2.amazonaws.com/nlab

Consistency

Peano Axioms (from Peano Arithmetic) holds true in First Order Logic.

For example: Smoking: Many people smoke even though they know it is harmful to their health.

This is a formally inconsistent statement.

Goldbach's conjecture : maybe true. The search space and example space is exhaustive. *“Every even integer greater than 2 can be written as the sum of two primes.”*

Reference: http://nlab-pages.s3.us-east-2.amazonaws.com/nlab

How decidable is formal logic?

Zeroth order logic is decidable - boolean axioms (FOL without variables or quantifiers).

Decidability of **First order logic** and **Higher order logic** are **complex**.

$\forall$x, King(x) $\wedge$Greedy (x) $\Rightarrow$ Evil (x)

Temporal Logic

All of these can have sequents

to prove.

Reference: https://plato.stanford.edu/

- $\exists x(philosopher(x) \wedge F\, king(x))$
  Someone who is now a philosopher will be a king at some future time.
- $\exists x F(philosopher(x) \wedge king(x))$
  There now exists someone who will at some future time be both a philosopher and a king.
- $F\exists x(philosopher(x) \wedge F\, king(x))$
  There will exist someone who is a philosopher and later will be a king.
- $F\exists x(philosopher(x) \wedge king(x))$
  There will exist someone who is at the same time both a philosopher and a king.

Fuzzy logic

This is more complex of all

Substructural Logic and uses Algebraic Semantics.

Source: https://plato.stanford.edu/entries/logic-fuzzy/#AlgeSema

Requires Hypersequents, uses analytic calculii.

Example: **A glass of warm water (not hot nor cold)**

This is not a Boolean Logic - we expect the tautologies to be ranging between 0 and 1. (Probabilistic Markov Logic Networks)

About Universal Validity

Hilbert: Is there an algorithm which, given an effectively described theory, such as Peano Arithmetics, and a sentence ξ in the theory decides, whether ξ is or is not provable from the axioms?

Halting problem: Is there an algorithm (program) Halt(P, F) which, given a source code P of another program and its input file F, decides whether P halts on the input F ?

Gödel's Theorem: reducing from arithmetic to axiomatic system is not possible. The satisfiability problem for T ×Z is undecidable (a consequence of Gödel's incompleteness theorem).

Turing: There is no such algorithm. Therefore, the halting problem is undecidable.

-> There is no such Universally valid algorithm

Machine Learning and Automated Theorem Provers

More recently, the FOL statements are encoded, with terminal symbols represented as one-hot encodings

Siamese RNNs for FOL : https://arxiv.org/abs/1906.00180

Can neural nets learn logic?

The expressive power of Algebra and Categorical Grammars via SAT/SMT solvers provides opportunities to adapt the theory to practice using Neural Networks.

Definitions

Conjecture: a logical consequence of statements which are axioms and Hypotheses.

Language: a formal specification for describing conjectures, axioms and hypotheses.

Proofs: how and why conjectures follow from axioms and hypotheses.

Source: https://www.tptp.org/OverviewOfATP.html

Well formed formula

A well formed formula sequence of symbols from an Alphabet from a formal language.

Proofs are often represented as sequences of such formulas to prove a final formula in the sequence.

$\forall x.\ P(x) \land \exists y.\ Q(y, f(x)) \lor \exists z.\ R(z)$

Each of the “term” P(x), Q (y, f (x)) and R(z) are **atoms** and are simplest of well formed formulas in logic.

Coalgebra

Topics

Coalgebra

Category Theory

Categorical Grammar

Coalgebra

Coalgebra represents a Duality space.

Coalgebra[F[_], A] - **A mapping from Abstract Data Type to functions space.**

Example: Matryoshka dolls problem - mapping tiniest to largest and vice versa. (Dual)

Frobenius Algebras:

The Frobenius algebras enable us to work in a single space in which meanings of words, phrases, and sentences of any structure live.

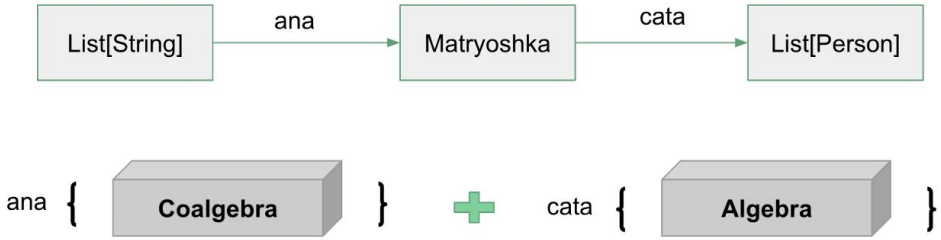
There is Duality in logic. - Anamorphism & catamorphism.

Ref: https://www.cs.ox.ac.uk/files/5468/sadrzadeh_kartsaklis.pdf

Coalgebra - example

Coalgebra

List	Matryoshka
[a, b, c, d]	Doll(a, [b, c, d])
[b, c, d]	Doll(b, [c, d])
[c, d]	Doll(c, [d])
[d]	Tiny(d)



ana

Fix(Doll(a,Fix(Doll(b,Fix(Doll(c,Fix(Tiny(d))))))))

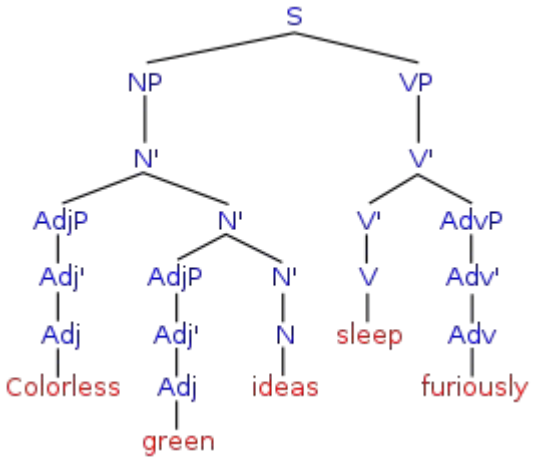
https://medium.com/@wiemzin/getting-started-with-recursion-schemes-using-matryoshka-f5b5ec01bb

Category theory

For describing the general abstract structures

Focuses on relations between objects than elements

Formal verification



Reference: http://nlab-pages.s3.us-east-2.amazonaws.com/nlab

Categorical Grammar

Categorical Theory

↓

Categorical Grammar

↓

Pregroup Grammar

↓

Lambek Syntactic Calculus

$$John : N \qquad Mary : N \qquad the : N \cdot N_0^l \qquad dog : N_0 \qquad cat : N_0$$

$$met : N^r \cdot S \cdot N^l \qquad barked : N^r \cdot S \qquad at : S^r \cdot N^{rr} \cdot N^r \cdot S \cdot N^l$$

$$N \cdot N^r \cdot S \cdot N^l \cdot N \leq S \cdot N^l \cdot N \leq S$$

$$\underset{N}{John} \quad \underset{N^r \cdot S \cdot N^l}{met} \quad \underset{N}{Mary}$$

A pregroup grammar consists of a lexicon of words (and possibly morphemes) L, a set of atomic types T which freely generates a pregroup, and a relation : that relates words to type.

Example

Statement 1: Colourless green ideas sleep furiously,

Statement 2: Pointless new ideas die rapidly.

Chomsky–Schützenberger enumeration theorem connects theory of formal languages and abstract algebra.

Reference:

1. https://www.math.mcgill.ca/barr/lambek/pdffiles/Pregrammars.pdf
2. Chomsky–Schützenberger enumeration theorem
3. http://nlab-pages.s3.us-east-2.amazonaws.com/nlab

SAT and SMT Solvers

Topics

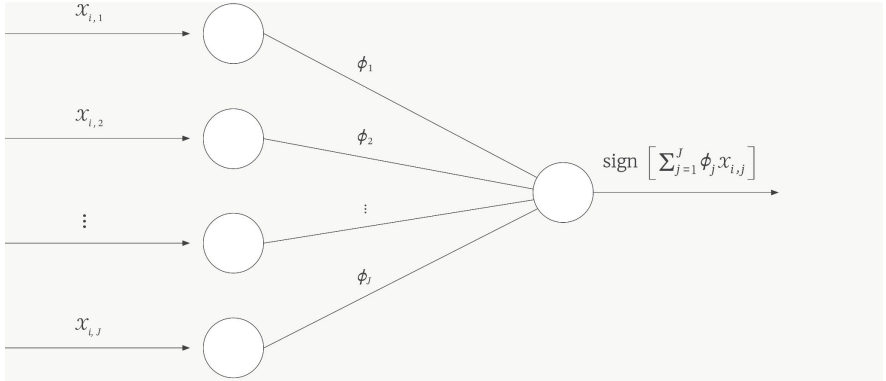
SAT Solvers

SMT Solvers

SAT Solvers

Boolean Satisfiability problem

- Convert to Conjunctive Normal Form
- Boolean satisfiability problem
- SAT problem in FOL is undecidable



Natural Language Beliefs and Logic Statements

- Let us say, we have following beliefs from previous slide:
  - Smoking causes cancer
  - Friends have similar habits
  - Let Alice and Bob be two friends
  - Alice Smokes and has Cancer
  - Alice has Smoking habit
  - Bob has Smoking habit
  - Can Bob get Cancer?

FOL : Some possible worlds: Domain(Alice, Bob)

Possible worlds	smokes(a)	Cancer(a)	smokes(b)	Cancer(b)	Friends(a,b)	Model
1	0	0	0	0	1	True
2	0	1	0	1	0	False
3	1	0	1	0	1	True
						SAT#: 2

SMT Solver

satisfiability modulo theories (SMT)

- To create verification engines that can reason natively at a higher level of abstraction
- Use First Order Logic
- The set of terms are freely generated from the set of variables and constant symbols.
- A theory (defined by set of sentences) over formulas is
  - Valid
  - Satisfiable if Entailment is satisfied
  - Not Satisfiable if Entailment is empty

SMT Theory

Validity and Satisfiability Modulo Theories

A *theory* is a set of sentences. For a given signature Σ, a Σ-*theory* is a set of sentences, each of which is a Σ-formula.

We will assume for convenience that theories are *closed under logical implication*.

Given a Σ-theory T, a Σ-formula ϕ is

1. T-*valid* if $\models_M \phi[s]$ for all models M of T and all variable assignments s.
2. T-*satisfiable* if there exists some model M of T and variable assignment s such that $\models_M \phi[s]$.
3. T-*unsatisfiable* if $\not\models_M \phi[s]$ for all models M of T and all variable assignments s.

http://theory.stanford.edu/~barrett/pubs/BT18.pdf

Why we might want to think of FOL and Formal verification for NL?

Topics

Natural Language

FOL

Formal Verification

Process of proving or disproving correctness of the algorithms, theories.

```
x = Int('x')
y = Int('y')
s  = Solver()
s.add(x >= 0)
s.add(y >= 0)
z = x + y
s.add(z == 0)
print(s)

print(s.check())
print(s.model())
```

```
[x >= 0, y >= 0, x + y == 0]
sat
[y = 0, x = 0]
```

Natural Language

Pregroup algebras can formalize grammatical Structure of Natural Language.

This structure is proven to be “implicit” in distributional model of word meaning based vector spaces, which applies to Word vector spaces.

We know that this can be satisfiable or not under Formal verification.

Why FOL if Language structure is already preserved?

To understand line of reasoning more formally

To formally verify if the line of reasoning is indeed satisfiable or not

Cover Entailment Relations

Topics

SAT Solvers

SMT Solvers

Findings relevant to Entailment Relations from the Book “Applied Combinatorics, by Fred S. Roberts & Barry Tessman”

- There exists a Maximum Matching M such that there is a K which is a minimum cover, then |M| = |K| . If = {x,y} and is in M then either x or y is in K.
- More formally, Cover is a topology such that cover of a set X is a collection of sets whose union includes X as a subset.
- Set cover problem has been np-complete since 1972.
- Universe: Consider the universe U = {1, 2, 3, 4, 5} and the collection of sets S = { {1, 2, 3}, {2, 4}, {3, 4}, {4, 5} }. Clearly the union of S is U. However, we can cover all of the elements with the following, smaller number of sets: { {1, 2, 3}, {4, 5} }.

Findings contd.

- This boils down to the set covering optimization problem: suppose there is a Universe U and family S of subsets of U, then the problem is there is a set of subsets k that are subsets of S that “covers” the Universe.
- Example: Bipartite graphs can be an example - A bipartite graph is a graph whose vertices can be partitioned into two disjoint sets that are independent of each other.
- This is part of a set of Problems known as Hitting Set problems.

Approach Description

The problem of the Cover in NLI problem lies at the intersection of Applied Combinatorics & Graph Theory.

The idea is suppose we have the “World Knowledge Graph” such as NELL: http://rtw.ml.cmu.edu/rtw/resources

and parse this knowledge graph by using a solution/algorithm to Entailment Cover relation problem.

Cover: NLI Entailment Relation

NLI Cover Entailment relations, animal vs non-apes - animal and non-apes have an 1) intersection of sets which is non-empty and 2) the union of the two subsets is Universal set. The point 2 matches with the Set Cover problem i.e. to find a minimum number of subsets in the {animal, non-apes} sets.

The Set and Graph theories do not consider “intersection” of subsets to be non-empty, as pointed out by Robert & Haris.

Solution: Set cover with Intersection size of at least 1

Name Change Suggestion: The name Cover needs to be changed since it is misleading with existing concept on Graph Theory/Combinatorics.

Q&A

Thank you!