1 FO-theories

Change of perspective:
Before: we were given a formula and had to check if it holds on a structure.
Now : We have a given structure what are the formulas that hold on that Structure

We are given a Structure
Theory $FO[U^S, R^S, \ldots, x^S, ..] =$ set of formulas ϕ that hold on the structure $S = (U^S, R^S, \ldots, x^S)$

$U^S =$ Universe
$R^S, \ldots =$ all relational Symbols
$x^S, \ldots =$ definition of free variables

1.1 Examples

Note: $' =' $ is always in the signature

1.1.1

$$FO[\mathbb{N}, <]$$

Use-case: is the structure with which one describes discrete,linear time.
NOTE: '<' is not a relational symbol but a real relation. The total order.
Contains the formulas:

$$\exists x(x = x)$$

meaning: tautology, maybe there is equality?

$$\forall x \exists y(x < y)$$

meaning: There follows a y after every x. Way to define infinity

$$\exists y \forall x \neg(x < y)$$

meaning: workaround to not define $>$ -> there is not just always a element bigger but also a element smaller than x

$$\forall xy(x = y \vee x < y \vee y < x) \ldots$$

meaning: the element is either equal,greater or smaller than x

1.1.1.1 Where did the free variables go?

As can be seen in the formulas above. There are no free variables. This is because there is not interpretation of free variables.

For instance if we have a formula:

$$\phi(x, y)$$

We do not know what values should be given to x and y. But there is a workaround!

We could insert every possible value for x and y in formula $\phi(x, y)$ from the universe and collect the results in a set like this:

$$\{(u,v) \in \mathbb{N} \times \mathbb{N} | (\mathbb{N}, <, x := u, y := v) \models \phi\}$$

The result of such an operation is not true or false but a set of objects which make the formula true.

We can also investigate all the sets that are defined by the formula i.e:

$$\phi(x,y) \underbrace{\rightarrow}_{\text{defines a}} \text{subset of } \mathbb{N}^2$$

example:
Are the prime-numbers definable in the theory $FO[\mathbb{N}, <]$?

Meaning: Is there a formula $\phi(\dots)$ that defines a set of exactly the prime numbers? (the answer is not in FO - First order logic only with < in the natural numbers, you need multiplication)

example:

$$f : n \rightarrow n + 1$$

Can we define f in the thory of $FO[\mathbb{N}, <]$
$?\exists\phi(x,y)$ st.

$$\{(u,v) \in \mathbb{N}^2 | (\mathbb{N}, <, x := u, y := v)\} \equiv \{(n, n+1) | n \in \mathbb{N}\} \equiv f$$

result:

$$\phi(x,y) = (x < y) \land \forall z \neg((x < z) \land (y < z))$$

meaning: the element y needs to be bigger than x and for all other numbers z they are not allowed to be bigger than x and be bigger than y.

Example:

$$f : n \rightarrow n + 1$$

Can we define f in the thory of $FO[\mathbb{N}, +1]$ where the $+1$ is $+1(n) = n + 1$ i.e. the successor function
Result: No it is not possible (he did not explain why)

We learn that $FO[\mathbb{N}, <]$ is more powerful than$FO[\mathbb{N}, +1]$ as we can not define a set that only contains $f : n \rightarrow n + 1$.

1.1.2 Presburg arithmetic:

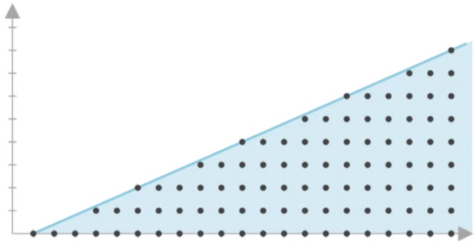
$$FO[\mathbb{N}, +]$$

- $\mathbb{N}$: Natural natural numbers
- $+$: ternary relation $+ \subseteq \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ i.e. $(i,j,k) \in + \iff k = i + j$

Applications:

- constraints solving
- theorem provers (Coq, Isabelle),
- distributed systems (Petri nets)

Example:



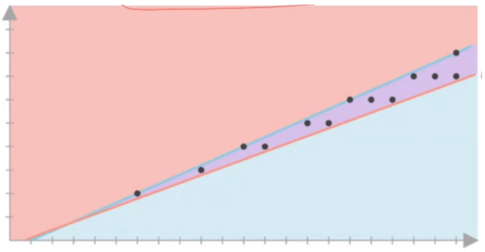
We can define a formula (see image above)

$$\phi_A(x,y) = (5 \cdot y <= 2 \cdot x - 2)$$

- But we have a problem how do we express multiply? By applying $+$ multiple times. For example: $5 \cdot y = y + y + y + y + y$
- And how do we express $<=$? We rewrite the formula to: $(5 \cdot y <= 2 \cdot x - 2) \iff \exists z(5x + z) = (2x - 2)$

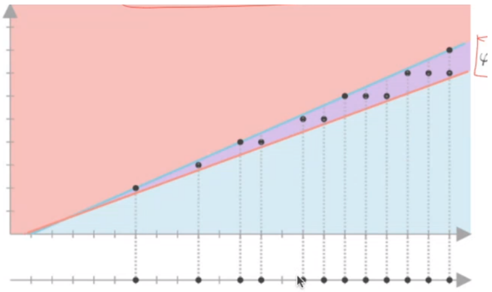
Or we define another formula and calculate its intersection:

$$\phi_B(x,y) = (9y >= 3x - 2)$$



And then we can calculate a projection on the y axis:

$$\phi_c(x) = \exists y \phi_{A \cap B}(x,y)$$



1.1.3 Peano arithmetic:

$$FO[\mathbb{N}, +, \cdot]$$

(sometimes undecidable (By reduction from Hilberts 10th problem, satisfiability of Diophantine equations), more powerful than Presburg arithmetic)

Question : How can this be undecidable if we reduced the $\cdot$ to $+$ in the Presburg arithmetic?

1.1.4 Tarski arithmetic:

$$FO[\mathbb{R}, +, \cdot]$$

- is Decidable even though it has more elements than Peano arithmetic.

Applications:

- Computer graphics: Splines,
- Invariants and abstractions, grammars equivalence,
- kinematics & motion planning, coding theory & cryptography

1.1.5

$$FO[\text{RadoGraph}]$$

1.1.5.1 What is a RadoGraph?

You distribute a infinite amount of nodes all over a surface. Then you throw a coin for all possible node pairs. If head you connect the two nodes. If tails you do not connect the nodes.

$$Pr[G \models \phi] \text{ as a function of nodes of } G$$

What doe this mean: G is a function of nodes that can either model ϕ or not.

Theorem:
If and only if the probability $Pr[G \models \phi]$ in a finite graph goes towards 1 it means that this formula G always models ϕ in an infinite graph .

Corollary 2 0 or 1 law for FO

- either $Pr[G \models \phi]$ tends to 1
- or $Pr[G \models \phi]$ tends to 0

This means that every FO - First order logic formula is

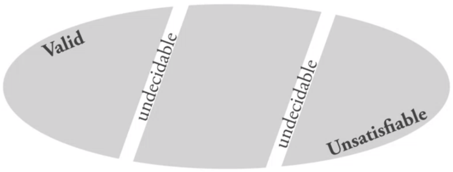
- either *almost surely true*
- or *almost surely false*

Examples:

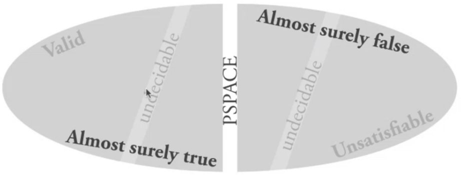
1. ϕ = 'There is a triangle' has $Pr[g \models \phi] \rightarrow 1$
2. ϕ = 'There is no 5-clique' has $Pr[g \models \phi] \rightarrow 0$
3. ϕ = 'There is a even number of edges' has $Pr[g \models \phi] \rightarrow \frac{1}{2}$

What can we deduct using Corollary 2 0 or 1 law for FO?
As 1. and 2. have the probability of 1 or 0 it means that we can write this property in FO - First order logic.
As 3. has a probability of $\frac{1}{2}$ we can not express this property with FO - First order logic.

If we have an overview over all formulas we can split them up into three parts. Valid, undecidable and unsatisfiable. Some formulas are always valid, for some formulas we can deduct they are never satisfiable (unsatisfiable) and sometimes we can not determine whether it falls into one class or the other i.e. it is undecidable as seen in the image below.



Now when we change our interest from *is the formula Valid or Unsatisfiable* to *is the formula almost surely true or almost surely false* in the sense that the probability is always 0 or 1 we can change the vendiagram from having three areas (Valid, undecidable, Unsatisfiable) to only having two areas (Almost surely true, Almost surely false). See image below



Brake

How do we compare our FO-theories?

2 Logical reductions

Recall: reductions!

A reduction from P to Q is an algorithm F that solves P using an oracle that returns solutions to Q.

Imagine P being easier than Q.

We transform Q to be easier. P should be easier afterwards using F

example:
many to one reduction: $\forall x, P(x) \iff Q(F(x))$

If we want to see similarities we can ask does the one theory reduce to the other theory?

Note: problems can be FO-theories
e.g

$$P = FO[S] = \{\phi : S \models \phi\}$$
$$Q = FO[T] = \{\phi : T \models \phi\}$$
$$\text{i.e. for all } \phi \quad S \models \phi \quad \iff \quad T \models F(\phi)$$

But as logician we do not like algorithms so F should not be a algorithm but we would like to define F using logic!

A Logical reduction is a specific case of a Algorithmical reduction

So what is our goal?
We want to automatically derive F from a logical description of S into T

A **Logical reduction**(reduction) of $\underbrace{S}_{FO[S]}$ into $\underbrace{T}_{FO[S]}$. is a mapping from relations R to S to multiple formulas α_R over T such that:

$$R^S \equiv \{\underline{u} : \quad T\underline{x} := \underline{u}] \models \alpha_R(\underline{x})$$

In easy words we express all relations of S using only the relations of T

For example:

We try to logically interpret $\underbrace{(\mathbb{N}, <)}_{S}$ into $\underbrace{(\mathbb{N}, +)}_{T}$. That means we express all relations of S using only relations of T :

$$\underbrace{\alpha_<(x, y)}_{S} = \underbrace{\exists z(y = x + z) \wedge \neg(y = x)}_{T}$$

Example 2:

Logical interpretation of $(\mathbb{Q}, <)$ into $(\{a, b\}^*, a, b, \cdot)$:

What do the relations mean:

- The universe of $\{a, b\}^*$ are strings a set of a and b i.e a, b, a, a, b
- $\cdot$ is the concatenation function $u \cdot v = w$ i.e. if you concatenate u and v you get the string w
- a and b are constants i.e. unary functions that do not require an input. for instance $u \cdot a = w$ means that if we concatenate a to u we get the string w

Question: how do we define which string has a higher value than another? Therefore we look at the following diagram.

Notes:

- ϵ is the empty string:
- if you take the left branch you add a a
- if you take the right branch you add a b
- We can traverse every tree. We use the In-order travers to define the order of the elements. In the diagramm of the visible elements are the order would be aa,a,ab,ϵ,b,ba,bb

It fulfills all properties of rational numbers for instance you can always find a rational number between two other rational numbers (between 2.1111 and 2.1112 is for instance 2.11115). In our description one just has to go down the tree. For instance between `ab` and `ba` there is `abb` which is bigger than `ab` and smaller than `ba`

$$\alpha_<(x, y) = \exists z, u, v \quad (x = z \cdot a \cdot u \wedge y = z \cdot b \cdot v) \vee (x = y \cdot a \cdot u) \vee (y = x \cdot b \cdot v)$$

meaning:

- $(x = z \cdot a \cdot u \wedge y = z \cdot b \cdot v)$ meaning:

  > Means that both x and y have a common ancestor z and are on the same level of the tree. For y to be bigger than x a 'b' has to follow z to create y.
  > Additionally a 'a' has to follow z to create x if we do not have this statement we would define a $=<$ as y and x could be equal.
  > as an example:
  > $x = aa, y = ab$
  > The common ancestor $z = a$
  > As we take the left branch to create x and the right branch to create y it follows that $x < y$.

- $(x = y \cdot a \cdot u)$ meaning:

> Is the case that y is a predecessor of x and to reach x one has to take a left brach. Hereby y has a higher value than x.
> As an example:
> $y = a$, $x = aa$
> As we have to go left on the tree after y to reach x. x has a smaller value than y.

- $(y = x \cdot b \cdot v)$ meaning:

  > x is a predecessor of y but why has a higher value as we have to take a right branch to reach y from x
  > As an example:
  > $x = b, y = bb$
  > x is smaller y as one has to take a right branch to reach y from x

Lets revisit our goal:
We want to automatically derive F from a logical description of S into T

But what does automatically mean?

Let say we have a formula ϕ over S and we want to logically reduce it to a formula $F(\phi)$ over T i.e.

$$\phi \text{ over } \underbrace{S} \to F(\phi) \text{ over } T$$

For instance:

> $\phi \text{ over } S = (x < y)$
> We need to replace '<' by $\alpha_<(x, y)$ over T i.e.
> $\phi \text{ over } T = \alpha_<(x, y)$