Lecture 2

Plan

- Review
- Presburger arithmetic
- Sets and relations

Presburger Arithmetic

Motivation

```
res = 0
i = x
while invariant res + 2*i == 2*x
  (i > 0) {
   i = i - 1
   res = res + 2
}
assert(res == 2*x)
```

Verification condition showing loop inv. preserved

$$res + 2\,i = 2\,x \;\wedge\; i1 = i - 1 \;\wedge\; res1 = res + 2 \rightarrow res1 + 2\,i1 = 2\,x$$

Proving integer linear arithmetic formulas

Verification condition showing loop inv. preserved

$$res + 2\,i = 2\,x \;\wedge\; i1 = i - 1 \;\wedge\; res1 = res + 2 \rightarrow res1 + 2\,i1 = 2\,x$$

Need to show it is true for all variables

Show: negation is never true (unsatisfiable)

$$res + 2\,i = 2\,x \;\wedge\; i1 = i - 1 \;\wedge\; res1 = res + 2 \;\wedge\; res1 + 2\,i1 \neq 2\,x$$

Here: substitute variables

$$(res+2) + 2(i - 1) \neq res + 2\,i$$

group coefficients – obtain “false”

Another Example

$\exists$ x,y,k,p.

$(x < y + 2 \wedge y < x + 1 \wedge x = 3k \wedge$

$(y = 6p+1 \vee y = 6p-1))$

Is this statement true?

General question:

is a formula of **Presburger arithmetic** satisfiable?

$F ::= A \mid F_1 \wedge F_2 \mid F_1 \vee F_2 \mid \neg F \mid \exists k.F \mid \forall k.F$

$A ::= T_1 = T_2 \mid T_1 < T_2$

$T ::= k \mid C \mid T_1 + T_2 \mid T_1 - T_2 \mid C \cdot T \mid T \,\%\, C$

Presburger arithmetic is decidable

There is an algorithm that, given arbitrary formula in the syntax of Presburger arithmetic, detects whether this formulas is satisfiable.

Thus also decidable are:

unsatisfiability, validity, equivalence, entailment.

Mojzesz Presburger. *Über die Vollstandigkeit eines gewissen Systems der Arithmetik.* Comptes rendus du I Congrès des Pays Slaves, Warsaw 1929.

Mojżesz Presburger (1904–1943) was student of Alfred Tarski and is known for, among other things, having invented Presburger arithmetic.

Method used: **quantifier elimination**

Quantifier Elimination

Take formula of the form

$\exists$ y. F(x,y)

replace it with an **equivalent** formula

G(x)

without introducing new variables.

Idea: eliminate quantified variables. E.g.

$\exists$k. x + k = 2 $\wedge$ k < 10

$\exists$k. k = 2 - x $\wedge$ k < 10 (one-point rule)

2 – x < 10

Arithmetic with only multiplication

Decidable. Use prime factor representation

$x = 2^{p1}\ 3^{p2}\ 5^{p3}\ 7^{p4}\ 11^{p5}\ \ldots$

$y = 2^{q1}\ 3^{q2}\ 5^{q3}\ 7^{q4}\ 11^{q5}\ \ldots$

$xy = 2^{(p1+q1)}\ 3^{(p2+q2)}\ 5^{(p3+q3)}\ 7^{(p4+q4)}\ 11^{(p5+q5)}\ \ldots$

Feferman-Vaught theorem: if we can decide logic of elements, we can decide logic of sequences of elements with point-wise relations on them.

Solomon Feferman (born 13 December 1928) is an American philosopher and mathematician with major works in mathematical logic. He was born in New York City, New York, and received his Ph.D. in 1957 from the University of California, Berkeley under **Alfred Tarski**. He is a Stanford University professor.

Alfred Tarski (January 14, 1901, Warsaw, Russian-ruled Poland – October 26, 1983, Berkeley, California) was a Polish logician and mathematician. Educated in the Warsaw School of Mathematics and philosophy, he emigrated to the USA in 1939, and taught and carried out research in mathematics at the University of California, Berkeley, from 1942 until his death.

… He is regarded as perhaps one of the four greatest logicians of all time, matched only by Aristotle, Kurt Gödel, and Gottlob Frege.

Formulas with both plus and times

- Posed as a big open problem at the beginning of 20th century to find decision procedure (Hilbert's 10th Problem)

Yuri Matiyasevich. *Enumerable sets are diophantine.* Journal of Sovietic Mathematics, (11):354 358, 1970.

Undecidability of Hilbert's Tenth Problem:

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

Summary

- Programs can be converted to formulas
- To prove program correct, we prove formula valid (true in all models)
- For some classes (e.g. Presburger arithmetic) we understand how to prove them
  - other classes – future research
  - such research can lead to tools that make software reliable