Lecture 16

Number Theory and Presburger Arithmetic

March 3, 1998
Lecturer: Richard Ladner
Notes: Jason Hartline

16.1. Continuing our look at the recursive inseparability of *CN*(**NT**) and *USAT*

We were in the process of proving the theorem that if $NT \subseteq \Gamma$ and Γ is consistent then *CN*(NT) is not computable.

Previously we defined two recursively inseparable languages L_1, and L_2 as

$$L_1 = \left\{\hat{T} \mid T \text{ halts and accepts } \lambda\right\}$$

$$L_2 = \left\{\hat{T} \mid T \text{ halts and rejects } \lambda\right\}$$

and made the claim that claim that *CN*(NT) and $USAT = \{\alpha \mid \alpha\neg\alpha\}$ are recursively inseparable. We will now finish the proof by reduction from L_1 and L_2. We will construct a formula φ_T with the properties:

1. NT $\models \varphi_T$ if T accepts λ
2. $\models \neg\varphi_T$ if T rejects λ

The number n will be used as a sequence of bits that represents a computation history T on input λ.

$$\begin{aligned}\alpha_T(n) &= pcomp_{\lambda,T}(n) \wedge (\exists p \leq n) D(p, n, \underline{A}) \\ &\quad \wedge \forall(m \leq n)\left[pcomp_{\lambda,T}(m) \rightarrow (\forall p \leq m)\neg D(p, m, \underline{R})\right]\end{aligned}$$

$\alpha_T(n)$ is true if T accepts λ. Here $pcomp_{\lambda,T}(n)$ is true if n represents a valid computation history of T on x (definition given last time). $D(p, m, d)$ is a predicate that means that the pth digit of n is d. In this case we use $\underline{A}$ and $\underline{R}$[1] for the accept and reject digit respectively.

[1] The notation $\underline{x}$ represents a constant that is not a free or quantified variable in the formula. $\underline{x} = \overbrace{ss\ldots s}^{x}0$ (the xth successor of 0)

$$\varphi_T = \mathrm{NT} \wedge \exists n \alpha_T(n)$$

$$\begin{array}{llll}
\hat{T} \in L_1 & \Rightarrow & \mathcal{N} \models \alpha_T(\underline{n}) & \text{for some } n \in \{0,1,\ldots\} \\
& \Rightarrow & \mathrm{NT} \models \alpha_T(\underline{n}) & \alpha_T(n) \text{ is bounded)} \\
& \Rightarrow & \mathrm{NT} \models \exists n \alpha_T(n) & \\
& \Rightarrow & \mathrm{NT} \models \mathrm{NT} \wedge \exists n \alpha_T(n) & \\
& \Rightarrow & \mathrm{NT} \models \varphi_T &
\end{array}$$

Now we will define $\beta_T(n)$ as true if n is a rejecting computation history.

$$\begin{array}{rcl}
\beta_T(n) & = & pcomp_{\lambda,T}(n) \wedge (\exists p \leq n) D(p, n, \underline{R}) \\
& & \wedge\ \forall (m \leq n) \left[pcomp_{\lambda,T}(m) \rightarrow (\forall p \leq m) \neg D(p, m, \underline{A}) \right]
\end{array}$$

$$\begin{array}{llll}
\hat{T} \in L_2 & \Rightarrow & \mathcal{N} \models \beta_T(\underline{n}) & \text{(for some } n \in \{0,1,\ldots\}) \\
& \Rightarrow & \mathrm{NT} \models \beta_T(\underline{n}) & \\
& \Rightarrow & \mathrm{NT} \models \exists n \beta_T(n) & \\
& \Rightarrow & \models \mathrm{NT} \rightarrow \exists n \beta_T(n) & \text{(deduction theorem)}
\end{array}$$

We can show using just the axioms about $<$ that

$$\mathrm{NT} \models \neg \left[\exists n_1 \alpha_T(n_1) \wedge \exists n_2 \beta_T(n_2) \right]$$

The three cases $n_1 < n_2$, $n_1 = n_2$, and $n_1 > n_2$ can be checked.

Let

$$N = \mathrm{NT}, \quad A = \exists n \alpha_T(n), \quad B = \exists n \beta_T(n)$$

From above we have

$$\begin{array}{l}
\models N \rightarrow B \\
\models N \rightarrow \neg(A \wedge B)
\end{array}$$

Using prepositional logic alone, we can conclude

$$\begin{array}{ll}
\models \neg (N \wedge A) & \\
\models \neg (\mathrm{NT} \wedge \exists n \alpha_T(n)) & \\
\models \neg \varphi_T & \text{by the definition of } N \text{ and } A
\end{array}$$

16.2. Presburger Arithmetic

We define Presburger Arithmetic model as

$$\mathcal{P} = (\mathcal{N}, s, +, <, 0)$$

where s is the successor function and $+$ and $<$ and 0 have their normal meaning over $\mathcal{N}$.

Theorem 16.1: *Th*($\mathcal{P}$) is decidable.

Proof: by elimination of quantifiers

First we will extend our model to include equivalence classes as follows:

$$\mathcal{PE} = (\mathcal{N}, s, +, <, 0, \equiv_2, \equiv_3, \equiv_4, \ldots)$$

Here, $x \equiv_m y$ means that $x - y$ is divisible by m. Note that if $\mathcal{PE}$ is decidable then so is $\mathcal{P}$ because we can have an expression for $\mathcal{PE}$ that does not have any of the equivalence relations and this would also be an expression in $\mathcal{P}$.

Let

$$\varphi = Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \alpha(x_1, \ldots, x_n)$$

where α is quantifier free. We will now show how quantifiers (and variables) can be removed starting with Q_n. We will rewrite φ without x_n. This can then be done repeatedly to eliminate all the quantifiers.

We will show that given an existential formula $\exists x \alpha(x_1, \ldots, x_{n-1}, x)$ we can construct an equivalent formula $\beta(x_1, \ldots, x_{n-1})$. That is, we construct a β such that for all $a_1, ..., a_{n-1} \in \mathcal{N}$

$$\mathcal{PE} \models \exists x \alpha(a_1, \ldots, a_{n-1}, x) \equiv \beta(a_1, \ldots, a_{n-1}).$$

The case of a universal quantifier reduces to the existential case because $\forall x \alpha(x_1, \ldots, x_{n-1}, x) \equiv \neg \exists x \neg \alpha(x_1, \ldots, x_{n-1}, x)$. Thus, we can construct β so that

$$\mathcal{PE} \models \forall x \alpha(x_1, \ldots, a_{n-1}, x) \equiv \neg \beta(a_1, \ldots, a_{n-1}).$$

There are a number of steps in eliminating the quantifier $\exists x$ from $\exists x \alpha(x_1, \ldots, x_{n-1}, x)$.

1. Remove negations:

$$\begin{aligned} \neg(t_1 = t_2) &\Rightarrow t_1 < t_2 \vee t_2 < t_1 \\ \neg(t_1 < t_2) &\Rightarrow t_2 < t_1 \vee t_2 = t_1 \\ \neg(t_1 \equiv_k t_2) &\Rightarrow \bigvee_{i=1}^{k-1} t_1 \equiv_k t + \underline{i} \end{aligned}$$

2. Simplify to conjunctions of atomic positive formulas (a.k.a. DNF conversion):

$$\exists x \alpha(x_1, \ldots, x_n, x) \Rightarrow \exists x \bigvee_{i=1}^{m} \bigwedge_{j=1}^{m} \alpha_{i,j}(x_1, \ldots, x_{n-1}, x)$$

Move the $\exists x$ inside the $\bigvee$. We now have:

$$\bigvee_{i=1}^{m} \exists x \bigwedge_{j=1}^{m} \alpha_{i,j}(x_1, \ldots, x_{n-1}, x)$$

Now, we just have to eliminate quantifiers of the form

$$\exists x(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_m)$$

where each α_i has the form where x is alone on one side of the equation, inequality, or congruence:

$$\begin{array}{ccc} nx + t = u & \xrightarrow{\text{rewrite}} & nx = u - t \\ nx + t \equiv_k u & & nx \equiv_k u - t \\ nx + t < u & & nx < u - t \\ u < nx + t & & u - t < nx \end{array}$$

Here, nx denotes n additions of x to itself. The terms t and u are linear combinations of the variables $x_1, \ldots, x_{n-1}$. For example, t and u have the form $j + \sum_{i=1}^{n-1} n_i x_i$, where j is a sum of constants and $n_i x_i$ is the sum of x_i with itself n_i times.

3. Solve for x. This means for all expressions α_i containing $n_i x$, find the least common multiple of n_i. Let p be the least common multiple, $p = \operatorname{lcm}(n_1, \ldots, n_{n-1})$, and let p_i be $\frac{p}{n_i}$ Then transform the statement $\exists x(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_m)$ to:

   $$\exists x(\alpha'_1 \wedge \alpha'_2 \wedge \ldots \wedge \alpha'_m)$$

   where

   $$\begin{array}{rcll} \alpha'_i & = & px < p_i u - p_i t & \text{if} \quad \alpha_i = n_i x < u - t \\ \alpha'_i & = & p_i u - p_i t < px & \text{if} \quad \alpha_i = u - t < n_i x \\ \alpha'_i & = & px = p_i u - p_i t & \text{if} \quad \alpha_i = n_i x = u - t \\ \alpha'_i & = & px \equiv_{p_i m} p_i u - p_i t & \text{if} \quad \alpha_i = n_i x \equiv_m u - t \end{array}$$

   Now, we need to make sure that the solution to this set of equalities, inequalities, and congruences is divisible by p and remove px from the expression entirely. To do this we will just add the congruence $x \equiv_p 0$ to obtain the equivalent formula

   $$\exists x \ (\alpha''_1 \wedge \alpha''_2 \wedge \ldots \wedge \alpha''_m \wedge x \equiv_p 0)$$

   where α'' is simply α' with x replacing px.

4. Special case with equalities: $x = u - t$ is in the conjunction. In this case, just substitute $u - t$ for x in the formula and add the clause $u - t \geq 0$.

5. Finally eliminate x: If we have no equalities then our formula looks like the following:

   $$\begin{aligned} \exists x \quad & [r_0 - s_0 < x \wedge \ldots \wedge r_{l-1} - s_{l-1} < x \\ & \wedge x < t_0 - u_0 \wedge \ldots \wedge x < t_{k-1} - u_{k-1} \\ & \wedge x \equiv_{m_0} v_0 - w_0 \wedge \ldots \wedge x \equiv_{m_{h-1}} v_{h-1} - w_{h-1}] \end{aligned}$$

   In this expression, the terms $r_i - s_i$ represent lower bounds on x. Every $r_i - s_i$ term could be negative of there may be no lower bound terms at all, so we add the inequality $r_l - s_l < x$

with $r_l = \underline{0}$ and $s_l = \underline{1}$ making -1 a strict lower bound. The $t_j - u_j$ represent upper bounds on choices for x. The least common multiple $m = \operatorname{lcm}(m_0, \ldots, m_{h-1})$ represents an spacing on which x must lie on. If there is a x on this spacing that is above all the lower bounds and below all the upper bounds. Then this part of the equation is satisfiable. Our final step is to rewrite as:

$$\begin{aligned}\beta \;=\; \bigvee_{i \leq l} \bigvee_{j<k} \bigvee_{1<q \leq m} \Bigg[& \bigwedge_{i' \leq l} (r_{i'} - s_{i'} \leq r_i - s_i) \wedge \bigwedge_{j'<k} \left(t_j - u_j \leq t'_j - u'_j\right) \\ & \wedge \left(r_i - s_i + \underline{q} < t_j - u_j\right) \wedge \bigwedge_{p<h} \left(r_i - s_i + \underline{q} \equiv_{m_p} v_p - w_p\right) \Bigg]\end{aligned}$$

Our decision procedure will be to remove all the quantifiers and then evaluate the final quantifier free formula. □

This quantifier elimination method has very high complexity. It can be shown by a different but related method that $Th(\mathcal{P}) \in SPACE(2^{2^{cn}})$.