Lecture 17

Ehrenfeucht Games and Bounded Quantifiers

March 5, 1998
Lecturer: Richard Ladner
Notes: Jayram S. Thathachar

In this lecture, we will consider the problem of deciding validity of first-order sentences in theories by bounding the range of the quantifiers in finite subsets. Suppose $Qx_1 \ldots Qx_n \alpha(x_1, x_2, \ldots x_n)$ is a first order sentence whose validity in needs to determined in some first-order theory. If we can bound the range of each of the variables x_i in some finite set, and still obtain an equivalent formula, then this problem becomes decidable. A technique that has proved useful for this approach is to analyze the validity of the formula using *Ehrenfeucht games*. As an illustration of this technique, we consider the first-order theory of arithmetic with only the less-than predicate, denoted by $\mathcal{N}_< = (N, <)$, and the decidability problem for sentences in $\mathrm{Th}(\mathcal{N}_<)$.

17.1. Ehrenfeucht Games

An Ehrenfeucht game is a 2-person game with players P_1 and P_2, and sets $S_1, S_2, \ldots S_n$, and $T_1, T_2, \ldots T_n$, each a subset of N. The game is played in n stages by P_1 and P_2 taking alternate turns with P_1 playing first. In the i-th stage, P_1 chooses to pick either a point $a_i \in S_i$ or a point $b_i \in T_i$. P_2 has to pick a point $b_i \in T_i$ in the former case, and a point $a_i \in S_i$ in the latter case. P_2 wins at the end of n stages if and only if for all $1 \leq i < i' \leq n$, $a_i < a_{i'}$ if and only if $b_i < b_{i'}$. The Ehrenfeucht game is good if P_2 has a winning strategy irrespective of the strategy used by P_1. For the problem of bounding the quantifiers, $S_i = N$ and $T_i = [0, B_i]$, for all i, where the B_i's are integers representing the bounds. For the rest of this section fix the sets S_i's and T_i's.

We formalize the notion that P_2 always has a winning strategy in the following way. For each k, we recursively define relations $\equiv_{k,n-k}$ between the sets $S_1 \times \cdots \times S_{n-k}$ and $T_1 \times \cdots \times T_{n-k}$. (These are not necessarily equivalence relations.)

For $k = 0$, $(a_1, \ldots, a_n) \equiv_{0,n} (b_1, \ldots, b_n)$ is true whenever $a_i < a_{i'}$ holds if and only if $b_i < b_{i'}$ holds for all $i < i'$. (This corresponds to the fact that at the end of the game P_2 has chosen the right set of points.)

For $k > 0$, $(a_1, \ldots, a_{n-k}) \equiv_{k,n-k} (b_1, \ldots, b_{n-k})$ is true whenever

$$(\forall a_{n-k+1} \in S_{n-k+1})(\exists b_{n-k+1} \in T_{n-k+1})(a_1, \ldots, a_{n-k+1}) \equiv_{k-1,n-k+1} (b_1, \ldots, b_{n-k+1}), \text{ and },$$

$$(\forall b_{n-k+1} \in T_{n-k+1})(\exists a_{n-k+1} \in S_{n-k+1})(a_1, \ldots, a_{n-k+1}) \equiv_{k-1,n-k+1} (b_1, \ldots, b_{n-k+1}).$$

This corresponds to the fact that P_2 must always have a move no matter what P_1 chooses to do. Note that when $k = n$, the relation $() \equiv_{n,0} ()$ implies that P_2 always has a winning strategy.

The simple but remarkable fact is that any formula with n quantifiers ranging over the S_i's is equivalent to the same formula with the quantifiers ranging over the T_i's. This is expressed in the more general lemma below by substituting $k = n$.

Notation: Denote

$$\mathcal{N}_<, x_1 = a_1, x_2 = a_2, \ldots, x_{n-k} = a_{n-k} \models Q_1 x_1 \ldots Q_n x_n \alpha(x_1, x_2, \ldots x_n)$$

by the simpler form

$$\mathcal{N}_< \models Q_{n-k+1} x_{n-k+1} \ldots Q_n x_n \alpha(a_1, \ldots, a_{n-k}, x_{n-k+1}, \ldots, x_n)$$

Lemma 17.1: Fix any k, $a_1 \in S_1, \ldots, a_{n-k} \in S_{n-k}$, and $b_1 \in T_1, \ldots, b_{n-k} \in T_{n-k}$. Then, $(a_1, \ldots, a_{n-k}) \equiv_{k,n-k} (b_1, \ldots, b_{n-k})$ if and only if for all quantifier-free formulas $\alpha(x_1, x_2, \ldots, x_n)$, and all quantifiers $Q_{n-k+1}, \ldots, Q_n$,

$$\begin{aligned} \mathcal{N}_< \models\ & (Q_{n-k+1} x_{n-k+1} \in S_{n-k+1}) \ldots (Q_n x_n \in S_n) \alpha(a_1, \ldots, a_{n-k}, x_{n-k+1}, \ldots, x_n) \\ & \leftrightarrow (Q_{n-k+1} x_{n-k+1} \in T_{n-k+1}) \ldots (Q x_n \in T_n) \alpha(b_1, \ldots, b_{n-k}, x_{n-k+1}, \ldots, x_n). \end{aligned}$$

Proof: Let $P(k)$ denote the statement of the lemma. The proof is by induction on k. When $k = 0$, there are no quantifiers. By the definition of $\equiv_{0,n}$, for all $1 \leq i, j \leq n$, $a_i < a_j$ if and only if $b_i < b_j$. Since $\alpha(x_1, \ldots, x_n)$ is equivalent to a Boolean combination of atomic formulas of the form $x_i < x_j$, then

$$\mathcal{N}_< \models \alpha(a_1, \ldots, a_n) \leftrightarrow \alpha(b_1, \ldots, b_n).$$

For the induction step, we assume that $P(k)$ holds and show below that $P(k+1)$ is true.

("only if"): Here we are assuming that $(a_1, \ldots, a_{n-k-1}) \equiv_{k+1,n-k-1} (b_1, \ldots, b_{n-k-1})$. By the definition of $\equiv_{k+1,n-k-1}$ and by the induction hypothesis $P(k)$, we have that for any $t \in T_{n-k}$, there exists a $s \in S_{n-k}$ such that

$$\begin{aligned} \mathcal{N}_< \models\ & (Q_{n-k+1} x_{n-k+1} \in S_{n-k+1}) \ldots (Q_n x_n \in S_n) \alpha(a_1, \ldots, a_{n-k-1}, s, x_{n-k+1}, \ldots, x_n) \\ \leftrightarrow\ & (Q_{n-k+1} x_{n-k+1} \in T_{n-k+1}) \ldots (Q_n x_n \in T_n) \alpha(b_1, \ldots, b_{n-k-1}, t, x_{n-k+1}, \ldots, x_n) \quad (17.1) \end{aligned}$$

Fix any $\alpha(x_1, x_2, \ldots x_n)$ and we are required to prove that

$$\begin{aligned} \mathcal{N}_< \models\ & (Q_{n-k} x_{n-k} \in S_{n-k}) \ldots (Q_n x_n \in S_n) \alpha(a_1, \ldots, a_{n-k-1}, x_{n-k}, \ldots, x_n) \\ \leftrightarrow\ & (Q_{n-k} x_{n-k} \in T_{n-k}) \ldots (Q x_n \in T_n) \alpha(b_1, \ldots, b_{n-k-1}, x_{n-k}, \ldots, x_n) \quad (17.2) \end{aligned}$$

It suffices to prove Equation 17.2 when Q_{n-k} is a universal quantifier since we can always negate both sides of the equivalence. So, assume that $Q_{n-k} = \forall$. We prove the forward direction of Equation 17.2; the other direction has a similar proof because of symmetry.

To prove this direction, fix any $t \in T_{n-k}$. By our earlier observation, there is an s satisfying Equation 17.1. Because we are assuming that the forward direction of Equation 17.2 is true, we can put $x_{n-k} = s$ to conclude that the premise of Equation 17.1 is holds. Therefore, the consequence of Equation 17.1 also holds. Since t was picked arbitrarily, the forward direction of Equation 17.2 follows.

("if"): Here we are assuming that for all $\alpha(x_1, x_2, \ldots x_n)$

$$\begin{aligned} \mathcal{N}_< \quad \models \quad & (Q_{n-k}x_{n-k} \in S_{n-k}) \ldots (Q_n x_n \in S_n)\alpha(a_1, \ldots, a_{n-k-1}, x_{n-k}, \ldots, x_n) \\ & \leftrightarrow (Q_{n-k}x_{n-k} \in T_{n-k}) \ldots (Q x_n \in T_n)\alpha(b_1, \ldots, b_{n-k-1}, x_{n-k}, \ldots, x_n) \end{aligned}$$

and we are required to prove $(a_1, \ldots, a_{n-k-1}) \equiv_{k+1,n-k-1} (b_1, \ldots, b_{n-k-1})$. The proof is left as an exercise. □

17.2. Bounding Quantifiers in $\mathcal{N}_<$

We will now give explicit bounds for the B_i's and prove that P_2 always has a winning strategy with respect to these bounds. Define

$$B_1 = 2^{n-1}, B_2 = 2^{n-1} + 2^{n-2}, \ldots, B_n = 2^{n-1} + \cdots + 2^0.$$

Let $T_i = N$ and $S_i = [0, B_i]$ for all i.

Lemma 17.2: $() \equiv_{n,0} ()$, i.e. P_2 always has a winning strategy.

Proof: We will show at in the stage with k moves left, whether P_1 picks a_{n-k+1} or b_{n-k+1}, P_2 can always choose some b_{n-k+1} or a_{n-k+1}, respectively, such that for all $1 \leq i < j \leq n-k$, $a_i < a_j$ if and only if $b_i < b_j$. We will actually maintain the following stronger set of invariants $I(k)$ (with $a_0 = b_0 = 0$): for all $0 \leq i < j \leq n-k$,

I1: $a_i < a_j$ if and only if $b_i < b_j$.

I2: $|a_j - a_i| < 2^k \Rightarrow a_j - a_i = b_j - b_i$.

I3: $|a_j - a_i| \geq 2^k \Rightarrow |b_j - b_i| \geq 2^k$.

We prove that $I(k)$ holds by downward induction on k. For $k = n$, $I(k)$ holds vacuously. Assume that $I(k)$ holds for $k \leq n$ and we want to now show that $I(k-1)$ holds. First, it can be verified that $I(k-1)$ holds whenever $i, j \leq n-k$ so we only need to verify the invariant when one of i or j is $n-k+1$. Suppose P_1 picks $a_{n-k+1} \in N$. (An analogous proof shows that $I(k-1)$ can be satisfied if P_1 picks $b_{n-k+1} \in B_{n-k+1}$.) We have the following cases of choosing b_{n-k+1} which depends on the range from which a_{n-k+1} was chosen.

Case 1: Suppose that $a_i < a_{n-k+1} < a_j$, for some i and j and for $\ell \neq i, j$, $a_\ell \notin [a_i, a_j]$ By the induction hypothesis no other b_ℓ lies in the interval, $[b_i, b_j]$ for $\ell \neq i, j$. Choose

$$b_{n-k+1} = \begin{cases} b_j - (a_j - a_{n-k+1}) & \text{if } a_j - a_{n-k+1} < 2^{k-1} \\ b_i + (a_{n-k+1} - a_i) & \text{if } a_{n-k+1} - a_i < 2^{k-1} \\ \left\lceil \frac{b_i + b_j}{2} \right\rceil & \text{otherwise} \end{cases}$$

(Observe that when $a_j - a_i < 2^k$, it is possible that both $a_j - a_{n-k+1} < 2^{k-1}$ and $a_{n-k+1} - a_i < 2^{k-1}$ are true but because of Invariant I2, b_{n-k+1} is still well-defined.

Case 2: Suppose that $a_i < a_{n-k+1}$ for all $i \leq n - k$. Let i be such that a_i is the maximum of all a_j, $j \leq n - k$. In this case, choose

$$b_{n-k+1} = \begin{cases} b_i + (a_{n-k+1} - a_i) & \text{if } a_{n-k+1} - a_i < 2^{k-1} \\ B_{n-k+1} & \text{otherwise} \end{cases}$$

We will not prove it here but it can be verified in each case that $I(k-1)$ holds. □

Corollary 17.3: $\mathrm{Th}(\mathcal{N}_<) \in \mathrm{PSPACE}(n^2)$. Moreover, it can be accepted by an alternating TM with n alternations and quadratic-time. To see this, the alternating machine follows the alternation of quantifiers using existenial moves for the existential quantifiers and universial moves for the universal quantifiers. In alternation i, the machine produces a number b_i in the range $[0, B_i]$. This number is of linear length in the formula. In the end the quantifier-free formula is checked for truth by substituting the b_i's for the variables x_i.