# Quantifier Elimination (continued)

Recall that in the last lecture we stated the problem of quantifier elimination:

We are given a boolean formula $\varphi$ in $s$ variables. Let $f_1, \ldots, f_s$ be $n$-variate polynomials of maximum total degree $d$ over an algebraically closed field $K$. Let $Q_1, \ldots, Q_w$ be quantifiers ($Q_i \in \{\forall, \exists\}$). And finally, let $x_1, \ldots x_n$ be $n$ variables divided into $w+1$ blocks $x^{[0]}, x^{[1]}, \ldots, x^{[w]}$. Note that $f_i(x_1, \ldots, x_n) = 0$ is a boolean variable whose value depends on $x_1, \ldots, x_n$. This boolean variable can be used as input to $\varphi$. Consider the following quantified formula:

$$F(x^{[0]}) = Q_1 x^{[1]} \ldots Q_w x^{[w]} \varphi(f_1(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0),$$

whose boolean value depends on the variables in the block $x^{[0]}$. Let $m$ be the number of variables in $x^{[0]}$. Output a boolean formula $\psi$ on $t$ variables and polynomials $g_1, \ldots, g_t$ in $m$ variables of degree at most $D$ such that

$$\psi(g_1(x^{[0]}) = 0, \ldots, g_t(x^{[0]}) = 0) = F(x^{[0]}).$$

In the last lecture, we dealt with a special case of this problem, when $w = 1$, $Q_1 = \exists$, and $\varphi = \wedge$. Then

$$F(x^{[0]}) = \exists x^{[1]} \bigwedge_{i=1}^{s} (f_i(x^{[0]}, x^{[1]}) = 0).$$

We saw that, using the Hilbert Nullstellensatz, we can transform $F$ into a quantifier-free formula of involving at most $(sd)^{n^2}$ polynomials in $n$ variables and of degree at most $(sd)^n$. Our goal is to apply that result to the general case, and obtain good bounds on $D$, the size of the output, and the running time of the computation.

## Handling Inequalities

The first generalization we are interested in is the case when we have both equalities and inequalities inside the AND. That is, $w = 1$, $Q_1 = \exists$, and $\varphi = \wedge$. Then

$$F(x^{[0]}) = \exists x^{[1]} (\bigwedge_{i=1}^{s_1} (f_i(x^{[0]}, x^{[1]}) = 0)) \wedge (\bigwedge_{i=1}^{s_2} (f_i'(x^{[0]}, x^{[1]}) \neq 0)).$$

We can reduce this to the already familiar case by using Rabinowitsch's trick. Let $y$ be a new variable and set $f = 1 - y \Pi_{i=1}^{s_2} f_i$.

$$F(x^{[0]}) = \exists x^{[1]} (\bigwedge_{i=1}^{s_1} (f_i(x^{[0]}, x^{[1]}) = 0)) \wedge (f(x^{[0]}, x^{[1]}) = 0).$$

Now we know how to eliminate the existential quantifier from here, and so we are done. Note that the maximum degree of the polynomials $g_1 \ldots, g_t$ we get by the procedure described in the previous lecture, is still at most $(sd)^n$.

## OR of ANDs with an Existential Quantifier

Now suppose the formula we are given is of the form:

$$F(x^{[0]}) = \exists x^{[1]}(\bigvee_{i=1}^{A} \varphi_i(f_1, ..., f_s))$$

where $\varphi_i(f_1, ..., f_s) = (\bigwedge_{j=1} s(f_j = 0) = A_{ij})$, where $A_j$ is just the truth assignment to the variables corresponding to each clause.

Note that the existential quantifier and the OR can trade places, and so we get:

$$F(x^{[0]}) = (\bigvee_{i=1}^{A} \exists x^{[1]} \varphi_i(f_1, ..., f_s))$$

Now, using what we have already seen, we can transform

$$\psi_i = \exists x^{[1]} \varphi_i(f_1, ..., f_s)$$

into formulas that do not involve quantifiers, on polynomials $g_1, ..., g_t$ of maximum degree $(sd)^n$. And so we get:

$$F(x^{[0]}) = \bigvee_{i=1}^{A} \psi_i(g_1, ..., g_t)$$

## Boolean Formula with One Existential Quantifier

When we are given a boolean formula on $s$ variables with an existential quantifier, we can examine all $2^s$ assignments to the variables and see which ones satisfy the formula. So potentially we can replace the formula with an OR of ANDs (DNF formula), where each AND clause specifies a truth assignment to the variables. This will introduce up to $2^s$ clauses.

Having this many clauses was something we wanted to avoid. However, it turns out that not all $2^s$ assignments to the variables are always realizable, by the following theorem, which is a derivative of the famous Bézout's theorem:

**Theorem 1** *Let $f_1, ..., f_s$ be polynomials of degree at most $d$ in variables $(x_1, \ldots, x_n)$. Let*

$$S = \{(I_1, ..., I_s) | \exists (x_1 \ldots, x_n) \ s.t. \ I_i = \text{“}f_i(x_1, \ldots, x_n) = 0\text{''}\}$$

*Then $|S| = O((sd)^n)$.*

By this theorem, we obtain two upper bounds on the number of clauses in the boolean formula where the existential quantifier is removed: $2^s$ and $O((sd)^n)$.

The proof of the theorem is actually constructive and gives us an algorithm for removing the existential quantifier. We will omit it for now.

Each of the $\min(2^s, O((sd)^n))$ clauses in the quantified DNF formula we obtain is an AND of truth statements about $s$ polynomials $f_i$ of degree at most $d$. By what we have already seen, it can be replaced by a quantifier-free formula which is an OR of $\min(2^s, O((sd)^n))$ clauses on $(sd)^{n^2}$ polynomials of degree $(sd)^n$.

## Quantified Boolean Formula

**Theorem 2** *Suppose we are given a Boolean formula with $w$ quantifiers:*

$$F(x^{[0]}) = Q_1 x^{[1]} \ldots Q_w x^{[w]} \varphi(f_1(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0)$$

*We can eliminate the quntifiers to obtain a Boolean formula with $(sd)^{O(n^{2w})}$ clauses, in $\min(2^{sw}, (sd)^{O(n^{2w})})$ polynomials of degree at most $sd^{O(n^{2w})}$.*

**Proof** We will begin by examining a formula of the form:

$$F(x_1, \dots, x_k) = \forall z_1, \dots, z_l \exists y_1, \dots, y_m \varphi(f_1(x_i, y_i, z_i) = 0, \dots, f_s(x_i, y_i, z_i) = 0)$$

First, we rewrite $F(x_1, \dots, x_k)$ as

$$F(x_1, \dots, x_k) = \neg(\exists z_1, \dots, z_l(\neg \exists y_1, \dots, y_m \varphi(f_1(x_i, y_i, z_i) = 0, \dots, f_s(x_i, y_i, z_i) = 0)))$$

Then, we eliminate the existential quantifier inside and obtain a formula of the form:

$$F(x_1, \dots, x_k) = \neg(\exists z_1, \dots, z_l(\neg \varphi'(g'_1(x_i, z_i) = 0, \dots, g'_{t'}(x_i, z_i) = 0)))$$

This formula has one quantifier, $O((sd)^n)$ clauses each involving $(sd)^{n^2}$ polynomials of degree at most $(sd)^n$. (The total number of polynimials is $O((sd)^{n^2+n}) = (sd)^{O(n^2)}$.) Now, we reiterate and remove the remaining quantifier, to obtain:

$$F(x_1, \dots, x_k) = \psi(g_1, \dots, g_t),$$

a formula that involves $((sd)^{O(n^2)} * (sd)^n)^n = (sd)^{O(n^3)}$ clauses, each on $((sd)^{O(n^2)} * (sd)^n)^{n^2} = (sd)^{O(n^4)}$ polynomials of degree $((sd)^{O(n^2)} * (sd)^n)^n = (sd)^{O(n^3)}$. By iterating this step, we obtain our bounds. ■

Thus we have seen that owing to Bezout's theorem, we can do quantifier elimination in time that is polynomial in the number of polynomials given. Next time we will talk some more about Bezout's theorem.